

BAPATLA ENGINEERING COLLEGE::BAPATLA

(Autonomous)

		N	IATI	HEM	ATI II E	CAL B. Te	FO	UND IV S	ATI emes	ONS ter	FO	R CY B401/	BER MA0	SEC	CURIT	Υ			
Le	ctures		:	2 Ho	urs/V	Veek]	utori	ial	:	1	Hou	r/We	ek	Practi	ical	:		0
CI	E Marl	ks	:	30			S	SEE N	Marks	s :	7	0			Credi	ts	:		3
Pr	e-Reg	uisite:	None	;															
Co	ourse (Object	ives:	Stude	ents v	will l	earn	how	to										
	\triangleright	Use I	Euclic	lean	and e	exten	ded 1	Eucli	dean	algo	rithn	ns to	find (GCD	of poly	nom	ials	s.	
	\triangleright	Appl	y var	ious 1	numt	ber th	eory	conc	epts	in sc	lvin	g con	gruen	ices.					
	\triangleright	Learn	ı how	v code	es in	math	emat	tics a	re use	ed fo	r err	or coi	rrectio	on an	d data	trans	smi	ssio	n.
	\triangleright	Cons	tructs	substi	itutio	n cip	hers	and t	transp	posit	ion c	ipher	·s.						
		1										1							
Co	ourse (20-1	Appl	nes: A y Eu nomia	After Iclide	study	ying 1 algor	this c ithm	ourse and	e, the	stud	lents d E	will I uclid	be ablee \overline{aan}	le to algori	ithm	to f	ind	GC	CDof
C	CO-2	Appl	v var	ious 1	numt	ber th	eorv	conc	epts	in sc	lvin	g con	gruen	ices.					
C	CO-3	Utiliz	ze lin	ear b	lock	code	s for	error	· dete	ctior	n and	corre	ectior	1.					
-	CO-4 Constructsubstitution ciphers and transposition ciphers																		
C	O-4	Cons	tructs	subsu	llulio	n cip	ners	and t	transp	oosit	ion c	ipher	S.						
C	.0-4	Cons	tructs	substi	itutio	on cip	oners	and	transp	posit	ion c	ipher	'S.						
C Ma	apping	of Cou	irse L	earni	ing O	utcoi	mes v	vith P	transp Progra	posit am C	ion c Dutco	mes d	[·] s. & Pro	gram	Speci	fic O	utc	omes	<u> </u>
Ma	apping	of Cou	irse L	earni	ing O	on cip	mes v	vith P	transp Progra O's	am C	ion c	mes d	^{·s.} & Pro	gram	Specif	fic O PS(utc D's	omes	<u> </u>
Ma	apping	of Cou	irse L	earni	ing O	utcon	mes v	vith P P(rogra O's	am C	on control	mes d	[·] s. & Pro	gram	Specin	fic O PS(2	utc D's	omes 3	5
Ma	apping C	of Cou	irse L 1 3	earni 2 3	ing O	utcon 4 -	mes v	vith P P(6 -	rogra D's 7 -	am C 8 -	001 C	mes d	•s. & Pro 11 -	gram 12 3	Specin 1 -	fic O PSC 2 3	utc D's	omes 3 -	
Ma	apping C C C C C C C C	of Cou 0 0-1 0-2	irse L 1 3 3	earni 2 3 3 2	ing O 3 2 2	utcor 4 -	mes v 5 -	vith P P(6 -	Progra D's 7 -	am C 8 - -	9 -	10 -	[·] s. & Pro 11 - -	gram 12 3 3 2	Specif 1 - -	fic O PS(2 3 3	utc D's	omes 3 - -	<u> </u>
Ma	apping C C C C C C C C C C	of Cou O D-1 D-2 D-3	rse L 1 3 3 3	earni 2 3 3 3 3	ing O 3 2 2 2 2	4 - -	mes v 5 - -	vith P P(6 - - -	Progr: D's 7 - -	am C 8 - - -	9 - -	10 - -	*s. & Pro 11 - - -	gram 12 3 3 3 3	Specif 1 - -	fic O PS(2 3 3 3 3	utco D's	omes 3 - - -	S
Ma	apping C C C C C C C C C C C C C C C C	of Cou O D-1 D-2 D-3 D-4	Irse L 1 3 3 2	earni 2 3 3 3 3 3	ing O 3 2 2 2 2 2	4 - - - -	mes v 5 - - - - - - - -	vith P P(6 - - -	Progra D's 7 - - - -	am C 8 - - - -	9 - - - -	10 	[·] S. & Pro 11 - - - -	gram 12 3 3 3 3 3	Speci 1 - - - -	fic O PSC 2 3 3 3 3 3	utco D's	omes 3 - - - -	5
	apping C C C C C C C C C C C	of Cou O D-1 D-2 D-3 D-4	Iructs Iructs I I I I I I I I I I	earni 2 3 3 3 3 3	ing O 3 2 2 2 2 2	4 - - - -	mes v 5 - - - UN	vith P P(6 - -	Progra D's 7 - - -	am C 8 - - -	9 - - - -	10 - - -	*S. & Pro 11 - - - -	gram 12 3 3 3 3 3	Speci: 1 - - -	fic O PS(3 3 3 3 ((utco D's	omes 3 - - - - Hou	s
C Ma	apping C C C C C C C C C C C C C C C C C C C	of Cou 0 0-1 0-2 0-3 0-4 0-4	rse L 1 3 3 2 xs In	earni 2 3 3 3 3 Nu	ing O 3 2 2 2 2 2 mber	•n cip •utcoi - - - - - -	mes v 5 - - - UN eory	vith P P(6 - - - VIT-1 and	Progra D's 7 - - -	am C 8 - - - -	9 - - - - Field	Image: Application of the second s	s. & Pro 11 Divis	gram 12 3 3 3 3 3 3	Speci 1 - - - y an	Fic O PSO 2 3 3 3 3 3 3 1	utco D's	omes 3 - - - Hou Div	rs)
Ma Ma Ba Al	CC CC CC CC CC CC CC CC CC CC CC CC CC	of Cou of Cou 0-1 0-2 0-3 0-4 0ncept n, The	rse L 1 3 3 2 s In e Euc	earni earni 3 3 3 3 Nui elidea	ing O 3 2 2 2 2 2 2 mber	•n cip •utcoi - - - - - - - - - - - - -	mes v 5 - - - - - UN eory	vith P P(6 - - - - - - - - - - - - - - - - - -	ransp Progra O's 7 - - - - - - - - -	am C 8 - - - - - Arit	9 - - - Field	10 	S. Pro 11 - - - Divis broups	gram	Speci 1 - - - y an	fic O PS(2 3 3 3 3 3 3 ((d T nd F	utco D's	omes 3 - - Hou Div:	rs)
Ba All Fie	apping C C C C C C C C C C C C C C C C C C C	of Cou O D-1 D-2 D-3 D-4 oncept n, The the for	rrse L 1 3 3 2 s In e Euc rm GI	earni earni 3 3 3 3 Nui elidea F(p),	ing O 3 2 2 2 2 2 mber n Al Poly	• Th lgorit nomi	mes v 5 - - - UN eory hm, al Au	vith P P(6 - - - VIT-1 and Mod	Progra D's 7 - - - - - - - - - - - - - - - - - -	am C am C 8 - - - - - - - - - - - - -	9 - - - - - - - - - - - - - - - - - - -	ID ID ID ID ID ID ID ID	& Pro & Pro 11 Diviss f the t	gram 12 3 3 3 s, Rin form	Speci 1 - - y an GF(2 ⁿ	Fic O PSC 2 3 3 3 3 3 1 0 1 </td <td>utco D's</td> <td>omes 3 - - Hou Div</td> <td>rs)</td>	utco D's	omes 3 - - Hou Div	rs)
Baa Al (So	apping C C C C C C C C C C C C C C C C C C C	of Cou O D-1 D-2 D-3 D-4 oncept n, The the for s 1 to 7	rrse L 1 3 3 2 s In e Euc rm GI v of C	earni earni 2 3 3 3 3 3 Nui elidea F(p),	mber n Al Polys	• Th lgorit in Te	mes v mes v 5 - - - - - - - - - - - - - - - - - -	vith P P(6 - - - VIT-1 and Mod rithmo	Progra D's 7 - - - - - - - - - - - - - - - - - -	am C am C 8 - - - Ariti Finit	9 - - - - - - - - - - - - - - - - - - -	ID ID ID ID ID ID ID ID	& Pro & Pro 11 Diviss f the t	gram 12 3 3 3 s, Rin form	Speci 1 - - y an GF(2 ⁿ	Fic O PSC 2 3 3 3 3 3 1 0 1 </td <td>utco D's</td> <td>omes 3 - - Hou Div:</td> <td>rs)</td>	utco D's	omes 3 - - Hou Div:	rs)
Ba Al Fic	CC CC CC CC CC CC CC CC CC CC CC CC CC	of Cou of Cou O D-1 D-2 D-3 D-4 oncept n, The the for s 1 to 7	rse L 1 3 3 2 s In Euc m GH	earni earni 2 3 3 3 3 3 Nui clidea F(p),	ing O 3 2 2 2 2 2 2 2 2 2 2 2 2 2	• Th lgorit in Te	mes v mes v 5 - - - - UN eory hm, al Ar extbo	vith P P(6 - - - - - - - - - - - - - - - - - -	Progra D's 7 - - - - - - - - - - - - - - - - - -	am C 8 - - - - - - - - - - - - - - - - - -	9 - - - - - - - - - - - - - - - - - - -	10 - - - - - - - - - - - - - - - - - - -	*S. & Pro & Pro - - - - - Divis f the f	gram 12 3 3 3 3 sibilit s, Rin form	Specit 1 - - y an GF(2 ⁿ	Fic O PSC 2 3 3 3 3 3 1 0 1 </td <td>(12</td> <td>omes 3 - - - - Hou Div: s, F</td> <td>rs) ision inite urs)</td>	(12	omes 3 - - - - Hou Div: s, F	rs) ision inite urs)
Baa Al Fice Ma	apping CC CC CC CC CC CC CC CC CC CC CC CC CC	of Cou O D-1 D-2 D-3 D-4 oncept n, The the for s 1 to 7 Numb	rse L 1 3 3 2 s In e Euc m GI y of C Der T	earni earni 2 3 3 3 3 3 Nui elidea F(p), thapt	mber n Al Polys er 3	• Th • Th lgorit in To Prime	mes v mes v 5 - - - - - - - - - - - - - - - - - -	vith P P(6 - - - - - Mod rithmod rithmod rithmod rithmod rithmod	ransp rogr: O's 7 - - - - I Fin ular etic, 1) 2 , Ferr	am C am C 8 - - - - - Ariti Finit	9 - - - - - - - - - - - - - - - - - - -	ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID	& Pro & Pro 11 - - - - Divis broups f the part of t	gram 12 3 3 3 sibilit, form	Specif 1 - - y an ngs ar GF(2 ⁿ	Fic O PSC 2 3 3 3 3 3 0 (d T nd F) rmat	utc D's	omes 3 - - Hou Div: ls, F 2 Hoo Theo	urs)
Baa Al, Fie (So Dec	apping CC CC CC CC CC CC CC CC CC CC CC CC CC	of Cou O D-1 D-2 D-3 D-4 oncept n, The the for s 1 to 7 Numl Fotient istic P	rse L rse L 1 3 3 2 s In c Euc m GI y of C per T Func Primal	earni earni 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 5 1 1 1 1	mber mber n Al Poly er 3 y: P Eul Algor	• Th • Th Igorit in Te • rime • rime	mes v mes v 5 - - - - - - - - - - - - - - - - - -	vith P P(6 - - - - - - - - - - - - - - - - - -	ransp rogra D's 7 - - - - - - - - - - - - -	am C am C 8 - - - - - - - - - - - - -	9 - - - - - - - - - - - - - - - - - - -	10 1 1 1 1 1 1 1 1	x Pro x Pro 11 - - - - - - - - - - - - -	gram 12 3 3 3 sibilit s, Rin form heore Mille inese	Speci 1 - - y an ngs ar GF(2 ⁿ em- Fe r-Rab Remain Remain	fic O PSC 2 3 3 3 3 3 3 3 3 3 3 3 7 7 7 7 7 7 7 7	utc D's	omes 3 - - - Hou Div: ls, F 2 Hoo Theo rithr Theo	urs) rrem, n, A rrem, n, A

(Sections 1 to 5 of Chapter 7 in Textbook 1)



BAPATLA ENGINEERING COLLEGE::BAPATLA

(Autonomous)

(12 Hours)

UNIT-3

Coding Theory:

Introduction to error correcting codes, Basic definitions, Matrix description of Linear Block Codes, Equivalent Codes, Parity Check Matrix, Decoding of a Liner Block Code, Syndrome Decoding,Error Probability after Coding, Perfect Codes, Hamming Codes, Optimal Linear Codes, Maximum Distance Separable codes.

(Sections 3.1 to 3.12 of Chapter 3 in Textbook 2)

	UNIT-4	(12 Hours)
· • • •		

Cryptography Basics:

Traditional Symmetric – Key Ciphers: Introduction, Substitution ciphers, Transposition ciphers.

(Sections: 3.1, 3.2, 3.3 of Text Book 3)

ı, 6 th
Tata Braw-
1 j