irstra	nker	's ch	ioice	www.FirstRank				Tim	w	ww.i	First		er.egm	Prin
3	<u>c</u>	<u>a</u>	· ©	9	(a)	ans		Time:3 hours]	CR	(SEA		per ID :	llow	Printed Pages: 3
Wha	Whi	Dist	Wh.	Wh	Spe	wer o		nuo	Ŕ	1.4			ing P	ages
What requirements should a digital signature scheme satisfy?	What are Message Authentication Codes (MACs)?	Distinguish between an active and passive attack	What is an authenticated Diffie-Hellman key agreement?	What is a stream cipher?	Specify two differences between procedural and object oriented language.	Attempt <u>all</u> parts. All parts carry equal marks. Write answer of each part in short. (2×10=20)		_	CRYPTOGRAPHY & NETWORK SECURITY	(SEM. VII) THEORY EXAMINATION, 2015-16		113702	Following Paper ID and Roll No. to Answer Book)	<u>ت</u>
uire: atisfy	Mess	sh bet	an au	strea	wo di ented	h part	SI		PHY	EOR			Ð	
nent:	age A	weer	then	m cip	ffere	All p	SECTION-A		& N	YE	B. Tech.	Roll No.[	nd R Answ	150
sho	uther	an a	ticat	her?	nces uage	arts o	-V	_	Ę	M	Ċ.	NZ E	er B	Ľ
uld a	ticati	ctive	<u>8</u> D		betw	any		Max	ORI	K		lН	o. to	
digi	on Co	and p	iffie		oen p	equal		MaximumMarks:100]	SEC	NOL		H	be fi	
ital s	des (	assiv	Helli		roced	mari (2		nMa	ÜRI	,201		ΙĦ	be filled in your	
igna	MA	e atta	nan		lural	arks. Write (2×10=20)		Ē	7	<del>5</del> 16		Н	in yo	EIT
ture	(s)?	Š.	key		and	vrite 20)		9				Н	Ĕ	EIT-701

EIL STLAUKEL COLU

www.FirstRanker.com

Ξ

P.T.O.

- (g) What type of security goals are used in cryptography?
- (h) Define S/MINE
- (i) What are the requirements for the use of a public key certificates scheme?
- (j) Explain briefly the two different approaches of Digital Signature?

## SECTION-B

Note: Attempt any five questions from this section.

operation?, What are the requirements of Message Authentication Code (MAC)? List and explain them. What are the properties of modular arithmetic (10×5=50)

What is Kerberos? Discuss Kerberos version 4 in Playfair Cipher with Key=DOLLARS. Encrypt the message "THIS IS AN EXERCISE" using

Chinese remainder theorem. of x for the following sets of congruence using the Define the Chinese remainder theorem? Find the values

X=2 mod 7 and X=3 mod 9

and decryption using RSA algorithm for What are the securities of RSA? Perform encryption

2

5400

3

EIT-701

p=17, q=11, e=7, m=88. EIT-701

> 7 Discuss the applications for public-key cryptosystems. What is the principle of public-key cryptosystems.

œ What are the properties of modular arithmetic

Define group field and finite field of the form GF(p).

## SECTION-C

Note: Attempt any two questions from this section

(15×2=30)

using the Chinese remainder theorem. Find the values of x for the following sets of Congruence

<u>.</u>

X=2 (mod 3)

X=1 (mod 4)

 $X=3 \pmod{5}$ 

Ξ

- decryption using RSA algorithm for p=11, q=13, e=7, Explain RSA algorithm. Perform encryption and
- the strengths of DES Draw block diagram of DES encryption. Also discuss

12.

×

www.FirstRanker.com