(08 Marks)

USN

Sixth Semester B.E. Degree Examination, June/July 2019 Cryptography, Network Security and Cyber Law

Time: 3 hrs.

Max. Marks: 80

Note: Answer any FIVE full questions, choosing ONE full question from each module.

	Note: Answer any FIVE Juli questions, Choose a	
	Module-1	(04 Marks)
1	a. Describe the types of Vulnerabilities to domain of security.	(04 Marks)
- 1	b List the guiding principles of segurity.	(08 Marks)
	c. Write the extended Euclidean algorithm, with an example.	(00 11441111)
	CA OP De	
-	Coloulete the value of vasing Chinese remainder theorem by given below data:	
2	11 010 - F n - 6 n - 1 X1 - 1 X2 - 3 A3 - 1	70
	Cinhar and the Hill (inner recinitions with inner recinitions)	(06 Marks)
	ttid diagram avalain kiestel stricture	(05 Marks)
	Module-2	(08 Marks)
3	a. Illustrate the RSA algorithm for encryption and decryption.	(04 Marks)
	b. Briefly explain the practical issues of RSA algorithm.	(04 Marks)
	c. List the properties of the cryptographic hash.	
	OR OF	(08 Marks)
4	a. Discuss the case study : SHA - I.	
	 a. Discuss the case study: SHA - 1. b. Explain the Man - In - the Middle attack on Diffie - Hellman key excha 	(08 Marks)
	diagram.	(00 1/2/2/20)
	Module-3	
	E 1: 1 P.C. A. Public Vary Infractructure (PKD) architectures	(08 Marks)
5	a di di 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	(08 Marks)
	OR	(DC Moule)
6	a. Explain the Kerberos message sequence with diagram.	(06 Marks)
	b. Describe the IP Sec protocols Authentication Header and Encapsulating Secur	ity ray load in
	transport mode.	(05 Marks)
	c. Explain Secure Sockets Layer (SSL) hand shake protocol.	(05 Marks)
	Module-4	
7	a. Explain the Authentication and Master Session Key exchange in 802.11i.	(05 Marks)
1	the state of the s	(05 Marks)
	The state of the s	(06 Marks)
	c. Explain Firewall functionality and Proxy life wall.	(00 marks)
	OR	
8	a. Write a note on Intrusion Detection System (IDS).	(05 Marks)
	b. Explain the types of Intrusion Detection System.	(05 Marks)
	c. Briefly explain the Technologies for Web Services.	(06 Marks)
	N. J. L.	
	Module-5 Evalois Digital Streeture Codification	Washington Town
9	a. Explain Digital Signature Certificates.	(10 Marks)
	b. Describe the duties of Subscribers.	(06 Marks)
	OR	
10	a. List any eight functions of the Controller.	(08 Marks)
	I wild to be the	(oo marks)

Briefly explain Penalties and Adjudication in IT Act.

Important Note: 1. On completing your answers, compulsority draw diagonal cross lines on the remaining blank pages.

2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

Vulnerabilities

- Weakness in a procedure, protocol, h/w or s/w within an organization that has the potential to cause damage.
- Vulnerability classes:
- 1. Human Vulnerabilities
- Induced by human behavior or action
- eg. clicking a link may leads to phishing or cross site scripting attack, e-mail virus

- 2. Protocol Vulnerabilities
- Protocols in LAN such as TCP, IP, ARP can be easily attacked
- Pharming attacks: ARP protocol to get passwords from LAN, man in the middle attack, replay attack

- 3. Software vulnerabilities
- In app' s/w
- eg
- Without validation of limit of user input may lead to buffer overflow
- in text field if some java script is given then validation is stopped eg of cross site scripting vulnerability
- in text field if SQL query is given then validation is stopped eg SQL injection vulnerability

- 4. configuration vulnerability
- configuration settings in newly installed s/w can be given wrongly e.g read, write & execute privileges

B. Guiding principles of security

Guiding Principles

- 1. Security is as much a human pblm than a technological pblm & must be addressed at different levels
- It should be addressed by top level mgmt

- Chief Information Security Officer (CISO)
 Robust security policies should be formulated
- Security Engineers
- key role to play in designing technique and products to protect organizations from the various cyber attacks
- System administrators
- Handle day-to-day operations
- Configure systems & applications
- Employees
- should be educated on various do's and don'ts through periodically updated security awareness programs.

2. Security should be factored in at inception, not as an afterthought

- Application s/w is often vulnerable to attack
- Soln: Integrating secure coding practices into the s/w curriculum in the colleges
- 3. Security by obscurity- unknown(or by complexity) is often bogus- not genuine or true
- New security protocols may also have serious vulnerabilities
- They should be properly deployed in hacker perspective

4. Always consider the "Default Deny" policy for adoption in access control

- Default Permit- unless subject(people, n/w packets.,,) is in Blacklist
- Default Deny unless subject is in Whitelist
- Disadvantages:
- Mistakenly some legitimate subject whose name has been excluded from the whitelist
- Mistakenly some attacker subject whose name has been excluded from the blacklist

- 5. An entity should be given the least amount/level of permissions/privileges to accomplish a given task
- Role based access control: principle idea in RBAC is that mapping between roles and permissions
- 6. Use 'Defense in depth' to enhance security of an architectural design
- 2 firewalls configured by 2 different s/m administrators

7. Identify vulnerabilities & respond appropriately

- Risk assessment
- Risk=Assests X Vulnerabilities X Threat
- If the assests impacted by a vulnerability are of low value and /or the threat perception(probability that a vulnerability is successfully exploited) is small, then the associated is low.
- In such case it may not make economic sense to address such vulnerabilities

c. Extended Euclidean algorithm

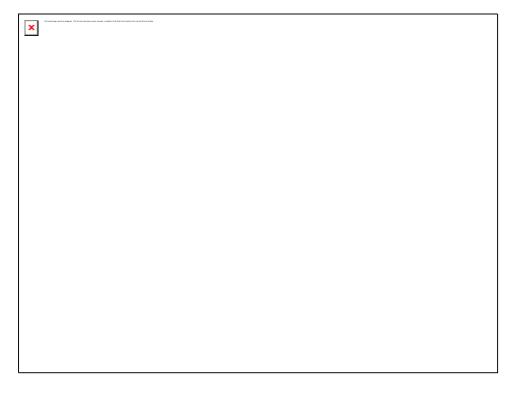
Extended Euclidean Algorithm

```
Algorithm: (inverse of c mod b)
computeinverse(b,c)
{
  old=1    new1=0
  old2=0    new2=1
  b'=b    c'=c
  r=2
  while(r>1){
```

```
q=b'/c'
r=b'%c'
temp1=old1-new1*q
old1-new1 new1=temp1
temp2=old2-new2*q
old2=new2 new2=temp2
b'=c' c'=r
new1*b+new2*c=r
}
return new2 //new2 is the modulo inverse
}
```

Extended Euclidean Algorithm > Used to find mod inverse > E.g: > b=79 c=12 inverse of 12mod79 > after iterations (-5)*79+33*12=1 > 12*33=1+5*79 ≡1(mod 79) > Thus the inverse of 12 modulo 79 is 33

2 Chinese Remainder Theorem



B Vignere Cipher and Hill Cipher

	Notice proof of page 1 to N as before const, usual and Administration of the state	
×		
		_
×	National and Administration constraints and the Administration and t	1
×		
×	Nationing agent agent. The United terminal, count of agent Unit (A) and A) grant to the address.	
×		
×	National and and an analysis of the second county county of the second county of the s	
×	National and Sub-Translations and a major to the Sub-Translation and the state of the Sub-Translation and Sub-	
×		
×		
×		
×		
×		
×		
×		
x		
x		
×		
×		
×		
×		
×		
×		
×		
×		

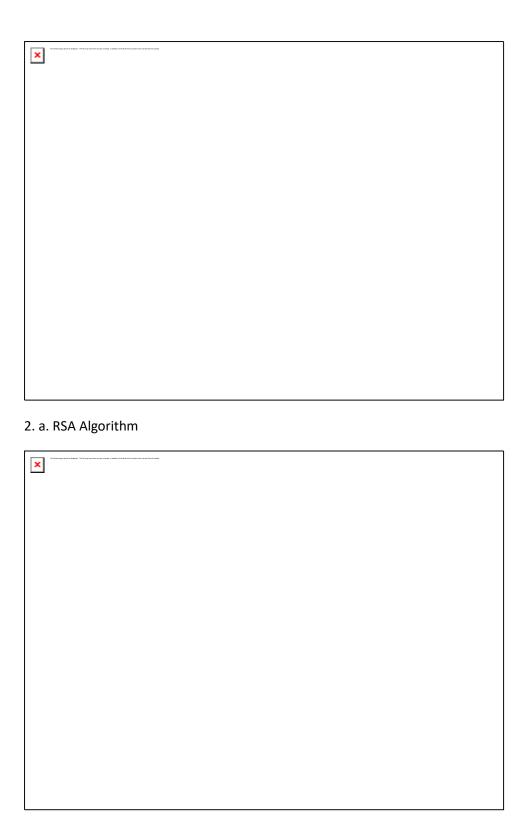
X Statemary contribution to the technological contribution of contribution of contribution of the contribu	

To bring inope cloud to digitized. To the may have been more	Lectured, or detailed. Yorky that the last participate correct the and decides.	
The Inflatinger second for displayed. The file may been force more	s, recurrent, or deleted, leafly that the left points to the current file and localise.	
The label image cannot be dudgingst. The file may have been more	, veneral, or delited, and y that the 3-depth in the current (to and location	
The latest language content for displayed. The file may been been record	, mones, or direct any find and an application care of the and insules.	
The Malating quantita diagonal. The Bit may have been received	, water, a state for the state to the state to the state to	
The Materiang current on diagnost. The for each bear bear section		
To intering works defined. So the significant contents of	. Amana a dana da hafa da da hafa da wa da mana	
** In the larger ward in depths. The file my has been con-	comment of more and the first and the second first mode.	
* In the consequence of the distribution of th		
An Automorphism & Alexan Table Inches Control	- comma - mass and half of the death of the formula	
The beautings are to date the best in the beautine control of the beautine con	. Command a desire del del del del del del del del del de	
An interconnect data in the inclusion control	command a manus and hard to the delection over the security	
* An Autoria and Age To De Inches and		
The bearings and the first Table to be the bearing and the first Table to the bearing and the bearing	communication and the first and the control for materials	
The bearings are to date. The De hydrocenters are	command a manus and half of the death has seen the mende	
* A harmony and it has "The British and and a second seco		
** An Australia Albania Tabu Barana Anna Anna Anna Anna Anna Anna Anna		
The bearings are to dead the best on the control of the best of th	Command a March of the Annaha and the Annaha and the Annaha and the Annaha and Annaha an	
* An Australia de Seria Parla		
As descriptions of the first based on the first based of the first based on the first bas		
The bearings and the first Table to be the bearing and the first Table to the bearing and	communication and the first and the second and the	
* Value of the second section of the second sec		
* An Australia Anna Table Anna Anna Anna Anna Anna Anna Anna Ann		
As descriptions of the description of the descripti		
* Value of the second section of the section of		
* An American and American Training and Amer		
As descriptions of the first terms of the first ter		
* Andrew and had be included in		
A bearing and have the broad control of the second of the		
X have good and have been account.		
* Andrew and Age To Be included in		
* And Annual Annual Technology of the Annual Technology of th		
X havenge and fine to be to be an account.		
* Shakeray and had be because on		
* Section of the Sect		
* Andrew and Ame To Be to be an account.		
As descriptions of the first terms of the first ter		

C. Feistel Cipher

_		
X		
_		
X	which had if two cold define it is the definite in the cold of the	
×	We have been been a series of the series of	
X To black in age	The Edge of Technique Council, and the Address of the Edge of Technique Council of Technique	
The Materimpe		
* Valuation of the state of the		
* Value of the state of the sta		
X		
X harry		
×		
×		
×		
×		
×		
× ·		
x		
x		
x		
X		
X		
x ·		
x		
x		
X		
X ·		
X The state of the		
x		
X The state of the		
X The state of the		
x ·		
X V		
X V		
X		

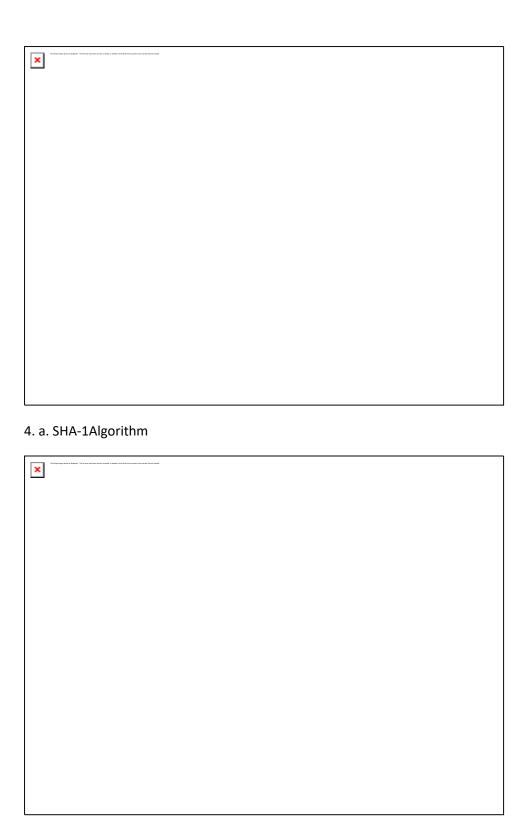
_		
X		
_		
X	which had if two cold define it is the definite in the cold of the	
×	We have been been a series of the series of	
X To black in age	The Edge of Technique Council, and the Address of the Edge of Technique Council of Technique	
The Materimpe		
* Valuation of the state of the		
* Value of the state of the sta		
X		
X harry		
×		
×		
×		
×		
×		
× ·		
x		
x		
x		
X		
X		
x ·		
x		
x		
X		
X ·		
X The state of the		
x		
X The state of the		
X The state of the		
x ·		
X V		
X V		
X		



	Notice proof of page 1 to N as before const, usual and Administration of the state	
×		
		_
×	National and Administration constraints and the Administration and t	1
×		
×	Nationing agent agent. The United terminal, count of agent Unit (A) and A) grant to the address.	
×		
×	National and and an analysis of the second county county of the second county of the s	
×	National and Sub-Translations and a major to the Sub-Translation and the state of the Sub-Translation and Sub-	
×		
×		
×		
×		
×		
×		
×		
x		
x		
×		
×		
×		
×		
×		
×		
×		
×		

The folial image cannot be adopted. The file may have been moved, variables, the delical, the file to be publicable control file and facilities.	
×	
-	
h Jesuas In DCA	
b. Issues In RSA.	
b. Issues In RSA.	
b. Issues In RSA.	
b. Issues In RSA.	

C. Properties of Hash function



	Notice proof of page 1 to N as before const, usual and Administration of the state	
×		
		_
×	National and Administration constraints and the Administration and t	1
×		
×	Nationing agent agent. The United terminal, count of agent Unit (A) and A) grant to the address.	
×		
×	National and and an analysis of the second county county of the second county of the s	
×	National and Sub-Translations and a major to the Sub-Translation and the state of the Sub-Translation and Sub-	
×		
×		
×		
×		
×		
×		
×		
x		
x		
×		
×		
×		
×		
×		
×		
×		
×		

	Notice proof of page 1 to N as before const, usual and Administration of the state	
×		
		_
×	National and Administration constraints and the Administration and t	1
×		
×	Nationing agent agent. The United terminal, count of agent Unit (A) and A) grant to the address.	
×		
×	National and and an analysis of the second county county of the second county of the s	
×	National and Sub-Translations and a major to the Sub-Translation and the state of the Sub-Translation and Sub-	
×		
×		
×		
×		
×		
×		
×		
x		
x		
×		
×		
×		
×		
×		
×		
×		
×		

×	To Management in playing it the first international control of the first international
^	
×	Name and a specific form of the specific form of th
×	To beginning search again. To the relation count of search and count of search to search count of search count of search to search count of search to search count of search to search count of
×	
x	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
×	
x	
×	
×	
×	
×	
×	
×	
×	

b. Man-in the middle attack

Man-in-the-Middle Attack

- 1. Darth prepares by creating two private / public keys
- 2. Alice transmits her public key to Bob
- Darth intercepts this and transmits his first public key to Bob. Darth also calculates a shared key with Alice
- Bob receives the public key and calculates the shared key (with Darth instead of Alice)
- 5. Bob transmits his public key to Alice
- Darth intercepts this and transmits his second public key to Alice. Darth calculates a shared key with Bob
- Alice receives the key and calculates the shared key (with Darth instead of Bob)
- Darth can then intercept, decrypt, re-encrypt, forward all messages between Alice & Bob

Man-in-the-Middle Attack Alice Mallory Bob A = g *mod p Z = g *mod p K_A = Z*mod p K_B = B*mod p K_B = B*mod p