08/08/23	DATE: / / PAGE NO.:
,	Mathematical Foundation for Blackshain
	[fSignment] /.
Summer!	It contradites hadifical charactus is it revolus in binary list
0/	What is cryptography. Differentiate between classial cryptography and modern
	(rypb graphy.
o algorithmy	(1) It is mately broad from search through (1) It relies on publicly house
Act	of codes so that only the authorized personnel can understand and process
10 1000	of codes so that only the authorized personnel can understand and process
	prople involved in communication land the steel for the firefit excepts
(II)	In (ryptography, the techniques which are used for protection are obtained from
	mathematical objects and a set of rules based calculations known as algorithmy
(20)	to convert messages in ways that are hard to decode
The Car	The algorithms are used for cryptographic key generation, digital signing, virification to protect data privacy, web browsing on internet and to protect
Prints	virification to protect and privacy, web browning on internet and to protect
	confidential bransactions.
(IV)	Advantages
Hull In	Acceptational primitive primitive formation of the various of the primitive looks and and acceptance of the primitive looks and the primitive looks and the primitive looks and the primitive looks are the primitive looks are the primitive looks are the primitive looks and the primitive looks are the primitive looks ar
	Cruptography can be used for access control to ensure that ends parties with the
	(ryptography can be used for access control to ensure that only parties with the proper paraissions have access to a resource. Only those with the correct
[anima]	dereription key can allew the resource.
	- STATES THE COMMITTEE OF A STATE OF THE COMMITTEE OF STATES OF ST
4.1	leure Communication videos is lossed as sudiente said
training of	For course online communication, cruptography is crucial. It offers sewe
	unechanisms for transmitting private information like passivoids, bank account
Daligne	numbers, and other junifive data over the internet.
Loglo	the programment during our ground thempered all
	Con Prolection against attacks williams industrialization
	(nyphography aids in defence against various kinds of avaults, including riplay and man-in-the-middle attack. It provides sharing for spotting and stopping
	and man-in-the-middle attack. It provides shategies for spotting and stopping
	these attacks

PAGE NO.:
Classical Cryptography Modern Cryptography
Humanit
(1) It manipulates traditional characters (vs It operates on binary bit requines.
(1) It manipulates traditional characters (vs. It operates on binary bit requires.
(11) It is mainly based on 'security through (11) It relies on publicly known algorithms
observity. The techniques imployed for for cooling. Secrety is obtained
mode involved in communication know the seed for the algorithm.
and buside about ithers in life our obtain superiod of subgrandary of the
maternatical concepts and a set of rules board calculations forces as objects
(111) 9+ requires the cohine cryptosystem (iii) Modern cryptography requires
for communicating confidentiality parties intinuted in secure communication
to possess the secret key only
Levishtani leilatile
(IV) Herminger
02 What are the various of cryptography primitives. Explain the role of these
primitive in cryptography.
THE SHE WAS LINE STATE OF THE S
A (I) (ryplographic primitives are the basic building blocks of a security protocol
or system. You will be an about cryptographic algorithms. These algorithms are crucial for creating safe protocols and systems. A
Jewity probed is a rules of actions made to use the proper security metanisms
in order to accomplish the necessary rewriter goals
(III) There are the low level algorithms that are used to build algorithms.
The programmers divilop new cryptographic algorithms with the help of
apprographic primitives.
Capagapay athe in defence against various diets of acception including many
(II) Role of primitives
(1) Searchy

DATE: / / PAGE NO.: 3
To viewe a honsaction in the ruturest or confidential information, strong
cryphography is required. So cruphographic primitives are used to durden
high-law agorimms. Which was a stranger of A
occurpaning behalque and superimeters to provide information sension
(n) Encryption and Decryption
The enyphographic primitives are used to divelop engiption and duryption algorithms
Energiption and duryption is done whenever required.
(11) Validation
The validation of data is done with the hilp of digital signatures. These digital signatures are public key primitives which the receivers use to validate the
mesage restriction princip toleran and attach sell is the
(iv) Spaific although antiques (a)
Cryphoraphic primitives are my spuific in nature. It means one cryphographic
primitive can parform only one function.
Cruphagraphic Aimitives
The state of the s
Kuy Leu Symmetric Kuy Augenmetric
Primitives Primitives Primitives
March March Digital Public
Random Mas II Ject 1 Construe Construe Construe
Numbers Functions Cropher Key Signatures Key Clones
Sheep Sheep
(1phics Ciphics
A delate version of the
The taxonomy of aryptographic primitives
The gifter to the value that a few all the party with the

Q3	Explain the various components of a basic cryptosystem.
to decile	supragely is equired to emphysical principles on und
A (I)	A cryptosystem is an implementation of cryptographic techniques and thur accompanying techniques and infrastructure to provide information successy
line for a death	A insplayation is also refirmed to as a cipher system.
appear (I) the en	(ryplayshms are used for sending musages in a secure manner over the
(111)	internet, such as credit card information and other private data.
	mino, sam as train and injunitarion and priess was
deal (TV)	Components of a Cryptosystim:
1401 2	Plaintex to the all reduce the parties are continued
(13	It is the data to be protected during harringsion
(11)	Emyption Algorithm (Cus)
- Magny qui	It is a mathematical process that produces a ciphertext for any given dointert
	and encryption key. It is a enployage hic algorithm that takes plaintext
	and an increption key as input and produces a ciphirket.
(111)	Ciphertext
time the	If is the trambled version of the plaintext produced by the encryption algorithm
130000	ding a key. The appoint is not quotate. It plous on public anoma.
A. De Dee	It is the crambbed version of the plaintext produced by the encryption aborithm using a key. The ciphertext is not guarded. It flows on public thoma! It can be interested or compromised by anyone who has access to the communication channel.
Public Via Gian	Associate English (sphalles)
(IV	A 1 A1 .11
	It is a mething tical process that produces a unique plaintext for any given
	appertext and disription key. It essentially reverses the encryption algorithm
	and is closely related to it.
	The franchist of American of the
(v) Enryption My
	The value known to the sonder that is used to compute the ciphertext for given

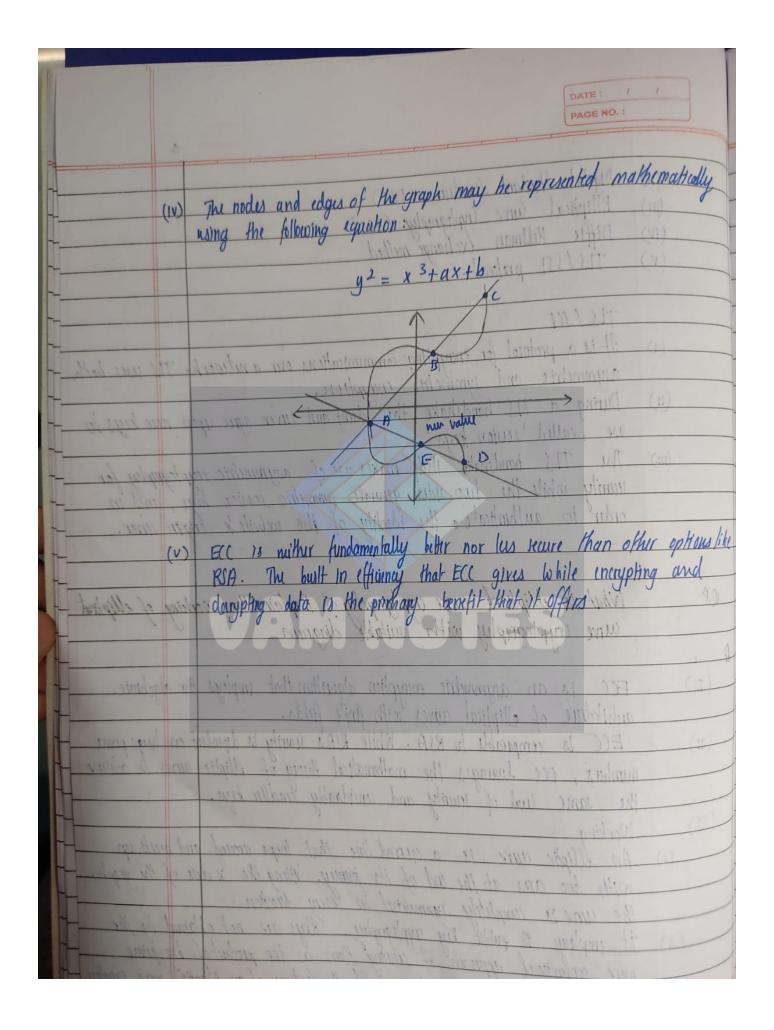
DATE: / /
PAGE NO.: 5
plainkx! .
(2) Of earlier side, engine during the apper test using his com it for
(vi) wolcopion key a sand about spanner will and open will be
The value known to the receiver that is used to decode the given ciphertext
into plainkxt. CAA) brandard cottopina brandard com
(a) Party Enemption Mankard (DES)
plainkx+ Encryption ciphuckx+ Decryption plaintx+
algorithm algorithm
(Riceins) Explish the various advantages and quadraguages (riber)
encryption key Intrueptor. duruption key
A feet About a land of the lan
Amilian with singular the sweeting of superior has
Ou What is symmetric key cryptography? Explain the working of symmetric key
cryptography with suitable diagram
A (I) Symmetric key cryptography is a type of encryption where a similar keys are
uxed to both encrypt and durypt nursages
9) 91 ix also known as shared-key, secret key, single key, one key and
workedly private key cryptography.
Roth the unit and receiver use common kus to encrypt and actives the
mirriage The seriet key is known only to the sender and to the receiver.
- An in and the continue for continue the transfer of continues
Norting Marking
displace to the test of the property of the or miles than bell the
plan level Engruption Computer to
(knder)
Arming phages on complet comments.
Defore sturking the communication, sender and receiver show the search key
(n) The serred key is shored through some external means.
(m) At sender sile, sender encrypts the manage using his copy of the key (w) The ciphus text is then sent to the receiver over the communication channel.
(v) 1W ciplus 10x+ 1x 10m scan per habitus xx 1 min from the first to the state of

	DATE: / / PAGE NO.:
	. Artainla
h-X	Al contracted receiver dements the cooper test using his cone of key
(v)	After duryphon. He musage converts back to restable format.
(W) cherty	ame encrusion algorithms and are
Tremple (mx)	(1) Advanced Encryption Standard (AES)
	(A) Nota Emploition (MINAURO (DE))
Mainley L	planter tengenter captures complete
	almillan almillan
0.5	Explain the various advantages and disadvantages of symmetric key
	algorithms. Adams of well assessed
A (=)	Advantages of symmetric key algorithms.
THE SERVENIE	Exerctional III VIII
(1)	Symmetric key encryption can be bighty source when it employe a source
No. of Street, or other party of the last	algorithm. AES is one of the most extensively used symmetric key corruption schemes.
(11)	Wing ten whother machines brute force questing the key using its
han and a	Wing ten pelaftop machines; brute force guessing the key wing its most source 256 bit length would take a billion years
	That are the training of the state of the st
A Ling (II) by	I speed the second on the second died (11)
1) min (i	It is putty simple to encrypt and decrypt symmetric by data
	resulting in excellent reading and writing performance
(11	Many SSDs, which are usually putty fast, use symmetric key
Figur Try I-	which don't use enuryption.
Carden	man sur rest supporte
(II)	Regulres low computer resources
(1	When compared to public key enception, single key encryption uses four
	computer resources.
	Minimizes millage (montonius
(I)	A distinct such that I've utilized for communication with each party,
	I wanted and I would be common with our party.

DATE: / /	
PAGE NO.: 7	f
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	H
preventing a wideplead musage security breaks	1
preventing a widepread musage security breach (ii) Only the musages sent by a specific pair of sender and receiver are affected if a key is compromised. Other people's communications are still safe.	0
The way is complained. Well proper communications are similare.	i
Deladvantaires of Summelvice alapin this many is tolive to	
Disadvantages of symmetric algorithms with the sound of authunitivity with singular	4
(1) Because both the sinder and receiver have the same key, minages cunnof	
Because both the sender and receiver have the same key, menages cumof be validated as coming from a specific user.	+
of encuption that was a pair of the in mayor and deport tothe	
(T) King Maring daylor with all sing a standard light of the self-	
(1) The most significant drawback of this is that the key must be communicated to the party with which you share data. (11) There muds to be a scurre method of delivering the key to the other purfy	
The party with which you make data.	,
(n) The mas to be a state memory of containing the and the fair	
Complex con January Mary Damage of Manuary	
(III) When two way communications are nary plad by symmetric encryption, both sides of the conversations are vulnowible.	+
sides of the conversations are vidnoable.	
Ca lamente uno policiva qui pritare tura cui	-
but Pluy won + alciphur numages sen 10 11 11 11 11 11 11 11 11 11 11 11 11	
encrypted with a diffirm they pour	
indetector wholeson	
06 Why 1x assymmetric key cryptography called public key cryptography	_
The state of the s	The same of the sa
A (T) The most significant advantage of using asymmetric by cryptography over	
symmetric encryption is the non-reliance on a single point of failure key	
(II) Since the key used to encrypt is already public, the key used to dicrypt the data is supposed to be private and need not be chared.	
$m \rightarrow m m m m m m m m m m m m m m m m m m$	ky
herning of its open nature	
Marine)	

	PAGE NO.:
(u)	This contrasts with symmetric encryption where the single key used for both encryption and decryption is supposed to be kept secret.
Q 7	What is asymmetric key cryptography? Explain the working of asymmetric key cryptography with suitable example
A (I)	Asymmetric encryption, also known as private key cryptography, ix a type
(I) (II)	and a private key which is kept suret by the owner. Accompanies configuration is realable for use in high and ever expanding
apud respons	environments where data are generally exchanged between diffirent communication partners. Asymmetric enjolography is used to exchange the secret key to prepare
	for using symmetric cryptography to energiption information
	Sinder Plaintext Encuptor Ciphered Data Decryption Plaintext Recon-
	public key privatekey
1010	All the data is cent through plaintext. It is then encrypted with a private public key. The ciphered data uses a private key to decrept
	11) It promotes seave key exchange which is a critical feature in naire
(E)	

DATE: / / PAGE NO.: 5	
Digital Shandard Signature & COUCH & washe how when we can	
(111) Elliptical Curve Cyphography (ECC)	
(IV) Diffie Hellman exchange method	
(v) TIS/SSI protocol+xxx+2 x = -1	- 1
-10/4	
TLS/SSL	. И.
asymmetric and symmetric encryption.	m
(11) During a TIS handshake, the client and server agree upon new keys h	6
we called review keys.	
(11) The TL(hand hake itself makes use of asymmetric cryptography for	
munity while the two sides generate symmetric session keys, and in	
order to authoriteate & the identity of the website is origin silver.	
(v) EXC 13 million fundamentally letter now too secure than other settles the	
as What is Minker curve compared to Explain the working of ellips	host
What is cliptical curve cryptography? Explain the working of ellips, with switable diagram.	
(I) Ecc is an asymmetric encryption algorithm that employs the algebraic architecture of elliptical curves with finite fields.	
ECC In comparable to RCA. While KIA's Constitut is abundant on higo orim	4
numbers FCC liverages the mathematical theory of elliptic curves to achie	ve
the same live of southly and considerably smaller keys.	
(III) Working (1) An elliptic curre is a curved line that loops around and much up	
and the area of the ord of its rolling. Along the X axis of the graph	4,
the wine is completely symmetrical in every direction. (1) It employes & eublic key cryptography. Keys are not obtained by the more consentional approach of creating them as the product of by prime nambers, but rather by taking use of the features of an elliptic wive equal to the features of an elliptic wive equal to the features of an elliptic wive equal to the features of the features of an elliptic wive equal to the features of the featur	
(1) It implays & public key cryptography. Keys are not obtained by the	
more conventional approach of creating them as the product of organice	a A
nambits, but rainir by taking use of the passing of	woh



For reference purposes only. Not liable for any misuse or misinterpretation.

We're interested in providing notes and assignments for free because college is more than just about submissions! :D Thank you for all your support!

Our repo - https://github.com/VAMNotes/VAMNotes (please star and share)

Our telegram - https://t.me/+Qva7WM1UEdc2YzNl

