

VASANTDADA PATIL PRATISHTHAN'S COLLEGE OF ENGINEERING & VISUAL ARTS

Page No. 0/

Experimento-ob sompton to other and en Aim-Implementation of coases Ciphen 1 # Theory - smalls assorts no dide of hallo QI Explain CIA security Modernal of codo - CIA security model also known as CIA Triad is a fundamental frame work in iformation security. Il stands for confidentially confidentiality. Integrity Confidentiality - This ensures that sensitive information is acressed only by authorized individuals. Techniques like encryption, across control, and authentication mechanism are used to maintain confidentiality. For example, using HTTPs for secure web browsing it ensures that the data transmitted between your browser and server remain confident. 11. Passive altock-Integrity - This ensure that the data remains accurate and unalterade during storage or transmission Integrity is maintained through method like checksum , hashing, digital signatures. The of a so monitoring backmission- The goal of opponent Availablity - This ensures that information and resources one acressible to outhonized user when needed. Avablity is maintain through redundancy, failover mechanisms, and regular maintainence. fore example, cloud services often uses multiple data centers to ensure that services remain ovoilable even if one data centre fails.

02 Explain different categories of attacks There are 2 types of attacks i. Active Attack- 10 mitotopologial and to Active attack are a type of cybersecurity attack in which on attacker attempts to alter ! destroy, or distrupt the normal operation of system or notwork report of a labora which of AD & Active attacks involve the attacker taking direct action against the target system or network and can be more dangerous. Types of active attacta Masquerade b. Modification, of message : c. Repudiation to be less so manager d. Replay and ATTH popul algraps to e. Denicul of Service 11. Passive attack-A passive attack attempts to learn or make use of information from the system but does not offect system resources. Passive attacks one in the nature of eavesdropping on or monitoring transmission. The goal of opponent is to obtain information, that is being od togosmitted adto a salesmo see more Types of passive attacksa. The release of message content b. Traffic analysis ata ecotors + corune that conjuce open



Cipher text

VASANTDADA PATIL PRATISHTHAN'S COLLEGE OF ENGINEERING & VISUAL ARTS

03. Explain Substitution Ceason Cipher Technique with modified Caesar Cipher Method as an Example

Substitution Cipher Method-A substitution cipher method of encryption where each letter in the plaintext is replaced with another letter. The substitution is based on fixed system, which is as simple as shifting letters by a certain number of position in the alphabets. 20 30022000 salt lappool of Example trated of copy text signal Plain Text-HELLOWA and brownsod abdudate Shifts + 3000 a grad) notized sulpu add tidal Cipher Text - KHOOR To break/decrypt the cipher text we need to replace the characters of cipher text message by aphabet 3 places back Modified Gaesar Cipher-

Modified Caesar Cipher—
To enhance the security of traditional ceaser Cipher In modified mesar cipher the alphaber in the plain text will not necessarily shif forward by 3 positions. It can be replaced by any other alphabet. Once the replacement scheme is decided it will be constant and will be used for all other alphabets in that message. There are 25 possibility for each alphabet

Example

Plain Text — Hello

Let Shift be 5

shift by 5 - Mo william not get shift by 5 mijodo cosoo halloga shift by 5 7 901 240 military Lighiff by 5 11-19 odg on shiff by 5, the color boo and ed a acitatitudus all mital mategia Alina in Hello - Miggt with askip bond as 1 10 radama Farition of ud apollat To decrypt the message we need to replace the characters of cipher text by alphabets backward the number of times we shif the value position (here 5 times backward) Copper Text - KHOOP to break I decaype the cipher text we need appearant the characters of appearant and molgan appoint a places about Modified Goscia Ciphon - 1 to appear the security of padifican course and and or redold of 25th worder construction of browset lide proposering ton this socially south uno und bosologe and got it anothers a on the replacement street is decided it will be stodada carta la cot ham ad thin has tappace and set philding so and and nonexy total



VASANTDADA PATIL PRATISHTHAN'S COLLEGE OF ENGINEERING & VISUAL ARTS

Q4	Explain Transposition Techniques with Simple Columnas Method as an example
	In this category Transposition technique no
	malanament or place tout material to done And
	preplacement or plain text content is done, only
	the position of the content of the plain text
	message is changed
	Simple Columnan Method-
	lets consider
	Plain Text - Everything is nothing
	Now write the plain text message now by
	row in a rectangle of pure defined size.
	lets consider the rectangle of 6 colums.
	The plain text will written as
	1 2 3 4 5 6
	EV. eryt
	h i n g i s
	nothin
	g and
	The American Concess of the Constitution of th
•	Now to encrypth this read the message
	rolumn by column in a random order of column
	column by column in a random order of column let's consider the order of column is - 2,3,6,5,4,1
	Our cipher text will be-
	vioent tsn yii rah ehna
	Vicentish directing
	everything is nothing - vioenttsnyiinghehng