D-40										1
Date	 		 *	*.*	• •	-	4	*	1	
Page										

Name: Avniba Dilubha Chudasma

Roll No: 07

*

TITLE: Assignment - I (ION)

Submitted To: Dr. Hardik Joshi

ASSIGNMENT-I

1. List all the Symmetric key Algorithms?

Ans * Symmetric key algorithm enoughtion is a type of incryption where only one key is used to both enought and decupt electronic information. It is used primarily for the bulk enoughtion of data or data streams. These algorithms are designed to be very just and have a large number of possible keys.

The best symmetric key algorithms offers excellent secrety, once data is encrypted with any given key; there is no jast way to decrypt the data without processing the same key.

Symmetraic key algorithme can be divided into two categories: block and stream. Block algorithms enought data a block (many bytes) at a time, while stream algorithms enought byte by byte (or even bit by blt).

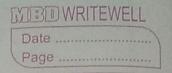
Commonly used Symmetric key algorithms are:

1. AES (Advanced Encryption Standard) or also known as Rijndael CAES): NIST selection for AES; developed by Daemen and Rijmen. It uses keys that are 128,192 or 256 bits long.

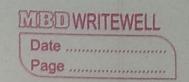
MBI	WRITEWELL
Date .	
Page	

- 2. DES C Data Enoughtion standard): was adopted as U.S government standard in 1977 and ANSI standard in 1981. It uses 56 bits long key.
- Blowfish: Block cipher developed by schmeier. It uses 1-448 bits long key.
- 4. IDEA (The International Data Encuption Algorithm) was block cyper developed by Massey and Xuejia. It uses 128 bits long key.
- 5. MARS: AES Finalist developed by IBM. It use key 128-256 bits long.
- 6. RC2: Block cipher developed by Ronald Rivest. Uses key of length 1-2048 bits.
- 7. RC4: Stream cipher developed by Ronald Rivest. It uses key of length 1-2048 bits.
- 8. RC5: Block cipher developed by Rivest and published in 1994 It was 128-256 bits length key.
- q. RC6: AES finalist developed by RSA habs. It uses key length of 128-256 bits.
- b. Triple DES: A three fold application of the DES algorithm.

 It used key length of 168 bits.
- 11. Serpent: AES Finalist developed by Anderson, Biham and Knudsen. It use key of 128-256 bit length.



Twofish: AES condidate developed by Schneley It isses 128-256 bits key length. 92 hist all the Asymmetric key algorithms? ans Asymmetric key encryption is based on public and private key encryption technique. It uses two different key to encrypt and decrypt the message. It is more secure than symmetric key encryption technique but is much slower Commonly used asymmetric key algorithms are: RSA algorithms (Rivest shamir Adleman)
Elliptic Curve Guyptography (ECC) Diffie - Hetlman key agreement. Digital Signature Algorithm (DSA) X25519 & X448 key exchange hist all algorithms jou Message digest 93 Message digest junctions distill the information Ans contained in a file (small or lærge) into a single lorge number typically between 128 and 256 bits in length. It rely on cryptography hash function to generale unique value. Commonly used Message digest algorithms one:



- 1. MD2 (Message digest #12) develop by Ronald Rivest · MD2 produces

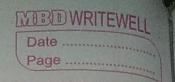
 a 128 bit digest.
- 2. MD 4 (Message digest #14) develop as jost alternative to MD4, it also produces 128 bit digest
- 3. MD5 (Message digest #5) produce 128 bit digest
- H. SHA Csecure Hash Algorithm) designed by NIST'S DSG and produces 160 bit digest
- 5. SHA-I (Revised Secure Hash Algorithm) more secure than SHA

 Produces 160 bit digest.
- 5. SHA-256) SHA-384, SHA-512 was proposed by NIST in 2001 Jou use in Advanced Encryption standard and used with 128-, 192-, and 256 bit encryption algorithms.

Assignment -2

- 1) Pisaus buiefly (one-two sentences)
- (a) PII (Personally Identifiable Information). is any data that could patentially identify a specific individual for example social security number (SSN) and driver license number etc.
- (b) US Ruivacy Act of 1974

 The privacy Act of 1974 (5 v.s. C 552 a) is a code of fair information pratices which mandates how federal agencies, such as the EPA, maintain records about individual.



- (0) FOIA (Erredom of Information Act) is a information daw that requires the full or partial discloser of previously unreleased information and documents controlled by United States government upon request
- (d) FERPA (The Family Education Rights Sand Privacy set of 1944)
 is a United States Jederal law that governs the access
 to education information and records by public entities
 such as potential employeers, publically Junded
 educational institute and Joseign government.
- (e) CFAA (The Computer Fraud and Abuse Act) is a United

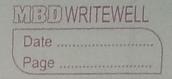
 States Cypersecurity bill that was enacted in 1986 as an

 someondment to existing computer information fraud

 law, which has been included in the Comprehensive

 cuine Control Act of 1984. It prohibits accessing a

 computer without authorization.
- (4) COPAA (The Council of Parent Attorney and solvocates) is an independent national American sussociation of parents of children with disabilities , actionneys, advocates, and related professionals who protect the legal and civil rights of students with disabilities and their family.
- (g) VPPA (Virtual sower surchase squeement) It is a contract in which the corporate buyer doesn't owns 2 mot responsible for the physical electrons generated by the project VPPA is purely financial transaction; exchanging a fixed price cash flow for a variable sized oash flow and renewable energy certificates (RECS)



(h) HIPAA (Health insurance Portability and Authority Act) It is a federal law that required the creation of notional standard to protect sensitive patients health information from being disclosed without the patients consent or knowledge

(i) GLBA (Gramm - heach - Bliley Act)

It is a US federal law that requires financial institution

to explain how they share and prefect their

customer private information

[j] PCI PSS (Payment Card Industory Data Security Standard)

It is standard for organization that handle bredit

cards from the major card schemes. It was created

to increase control around sand holder data to

reduce credit sand fraud.

(k) FCRA (Fair Gredit Reporting Act)

is a jederal law that regulates the collection of

Consumer credit information and access to their credit

information reports and protect privacy of the

personal information

It is an amendment to FCRA that was ended primarily to protect consumers from identity theft. The Act stipulates requirement for privacy information, privacy succuracy and disposal and limits the way consumer information is shared.