

Name : Arniba 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 encryption is a type of encryption where only one key is used to both encrypt and decrypt electronic information. It is used primarily for the bulk encryption of data or datastreams. These algorithms are designed to be very fast and have a large number of possible keys.
- * The best symmetric key algorithms offers excellent security, once data is encrypted with any given key, there is no fast way to decrypt the data without processing the same key.
 - * Symmetric key algorithms can be divided into two categories: block and stream. Block algorithms encrypt data a block (many bytes) at a time, while stream algorithms encrypt byte by byte (or even bit by bit).

Commonly used Symmetric key algorithms are:

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

2. DES (Data Encryption standard): was adopted as U.S government standard in 1977 and ANSI standard in 1981. It uses 56 bits long key.
3. Blowfish: Block cipher developed by Schneier. It uses 1-448 bits long key.
4. IDEA (The International Data Encryption Algorithm) was block cipher 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 uses 128-256 bits length key.
9. RC6: AES finalist developed by RSA labs. It uses key length of 128-256 bits.
10. 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.

Q2. Twofish : AES candidate developed by Schneier. It uses 128-256 bits key length.

Q2 list 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:

1. RSA algorithms (Rivest Shamir Adleman)

2. Elliptic Curve Cryptography (ECC)

3. Diffie - Hellman key agreement.

4. Digital Signature Algorithm (DSA)

5. X25519 & X448 key exchange

Q3 list all algorithms for Message digest

Ans Message digest functions distill the information contained in a file (small or large) into a single large number typically between 128 and 256 bits in length. It relies on cryptography hash function to generate unique value.

Commonly used Message digest algorithms are:

1. MD2 (Message digest #2) develop by Ronald Rivest. MD2 produces a 128 bit digest.
2. MD4 (Message digest #4) develop as fast alternative to MD2, it also produces 128 bit digest.
3. MD5 (Message digest #5) produce 128 bit digest.
4. SHA (Secure Hash Algorithm) designed by NIST's DSS and produces 160 bit digest.
5. SHA-1 (Revised Secure Hash Algorithm) more secure than SHA produces 160 bit digest.
6. SHA-256, SHA-384, SHA-512 was proposed by NIST in 2001 for use in Advanced Encryption standard and used with 128-, 192-, and 256 bit encryption algorithms.

Assignment -2

- (i) Discuss briefly (one - two sentences)
- (a) PII (Personally Identifiable Information): is any data that could potentially identify a specific individual for example social security number (SSN) and driver license number etc.
- (b) US Privacy Act of 1974
The privacy act of 1974 (5 U.S.C 552 a) is a code of fair information practices which mandates how federal agencies, such as the EPA, maintain records about individual.

- (10) FOIA (Freedom of Information Act) is a information law that requires the full or partial disclosure of previously unreleased information and documents controlled by United States government upon request.
- (11) FERPA (The Family Education Rights and Privacy Act of 1974) is a United States federal law that governs the access to education information and records by public entities such as potential employers, publically funded educational institute and foreign government.
- (12) CFAA (The Computer Fraud and Abuse Act) is a United States Cybersecurity bill that was enacted in 1986 as an amendment to existing computer information fraud law, which has been included in the Comprehensive Crime Control Act of 1984. It prohibits accessing a computer without authorization.
- (13) COPAA (The Council of Parent Attorney and Advocates) is an independent national American association of parents of children with disabilities, attorneys, advocates, and related professionals who protect the legal and civil rights of students with disabilities and their family.
- (14) VPPA (Virtual Power Purchase Agreement) It is a contract in which the corporate buyer doesn't own & not responsible for the physical electrons generated by the project - VPPA is purely financial transaction, exchanging a fixed price cash flow for a variable sized cash flow and renewable energy certificates (RECs).

- (h) HIPAA (Health Insurance Portability and Accountability Act) It is a federal law that required the creation of national standard to protect sensitive patients health information from being disclosed without the patients consent or knowledge
- (i) GLBA (Gramm - Leach - Bliley Act)
It is a US federal law that requires financial institution to explain how they share and protect their customer private information
- (j) PCI DSS (Payment Card Industry Data Security Standard)
It is standard for organization that handle credit cards from the major card schemes. It was created to increase control around card holder data to reduce credit card fraud.
- (k) FCRA (Fair Credit Reporting Act)
It is a federal law that regulates the collection of consumer credit information and access to their credit information reports and protect privacy of the personal information
- (l) FACTA (Fair and Accurate Credit Transaction Act)
It is an amendment to FCRA that was enacted primarily to protect consumers from identity theft. The Act stipulates requirement for privacy information, privacy accuracy and disposal and limits the way consumer information is shared.