Name :- Rajivadiya Parishita N.

Roll No :- 35

Course :- MCA - I

Assignment :- 1

1. List all symmetric key algorithms.

=> Answer :

-> Introduction of symmetric key

Symmetric encryption is a type of encryption where only one key is used to both encrypt and decrypt electronic information. The entities communicating via Symmetric encryption must exchange the key so that it can be used in the decryption process. This encryption method differs from asymmetric encryption where a pair of keys, one public and one private, is used to encrypt and decrypt messages.

By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original and understandable form. The secret key that the sender and recipient both use could be a specific password / code or it can be random string of letters or numbers that have been generated by a secure random number generator.

Page
Date

⇒ There are two types of Symmetric encryption algorithms:

1. Block algorithms:
Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.

2. Stream algorithms:
Data is encrypted as it streams instead of being retained in the system's memory.

Examples of Symmetric encryption algorithms

Block cipher :- Advanced Encryption standard
, Data Encryption standard.
, International Data Encryption Standard.
. Blowfish.
, Rivest Cipher 5.
, Rivest cipher 6.

Stream Cipher :- Rivest Cipher 4.

⇒ Conclusion :-
Maintaining large-scale symmetric encryption systems is very challenging task.

Page
Date

2. List all asymmetric key algorithms.

=> Answer:

-> Introduction:

Asymmetric Encryption, also known as Public-key cryptography. Unlike Symmetric encryption, Asymmetric Encryption encrypts and decrypts the datas using two seperate yet Mathematically connected cryptographic keys. These keys are known as a 'Public key' and a 'Private key'. Together, they're called a 'Public and Private key pair'.

Let's see how these two keys work together to creat the formidable force that is Asymmetric Encryption.

-> Algorithms:

Asymmetric Encryption uses two distinct, yet related keys. One key, the Public key, is used for encryption and the other, the Private key, is for decryption. As implied in the name, the Private key is intended to be private so that only the authenticated recipient can decrypt the message.

→ Example of well-regarded asymmetric key techniques for varied purposes include:

- Diffie-Hellman key exchange protocol.
- Digital Signature standard
- ElGamal
- Elliptic-curve cryptography
  - Elliptic Curve Digital Signature Algorithm
  - Elliptic-Curve Diffie-Hellman
- Various password-authenticated key agreement techniques
- Paillier cryptosystem
- RSA encryption algorithm
- Cramer-Shoup cryptosystem
- YAK

→ Examples of asymmetric key algorithms not widely adopted include:

- NTRUEncrypt cryptosystem
- McEliece cryptosystem

→ Examples of notable-yet insecure-asymmetric key algorithms include:

- Merkle-Hellman knapsack cryptosystem

3. List the algorithms for message digest

⇒ Answer:

→ Introduction:

Message digest is used to ensure the integrity of a message transmitted over an insecure channel. The message is passed through a cryptographic hash function. This function creates a compressed image of the message called digest.

⇒ ~~Example~~ List of message digest algorithms

- SHA3-512
- SHA-384
- SHA
- SHA3-384
- SHA-224
- SHA-512/256
- SHA-256
- MD2
- SHA-512/224
- SHA3-256
- SHA-512
- MD5
- SHA3-224

a) Personally identifiable information.

PII is any data that could potentially be used to identify a particular person. Examples include a full name, Social Security number, driver's license number, bank account number, passport number, and email address.

b) US Privacy Act of 1974.

The Privacy Act of 1974, as amended, 5 U.S.C., 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

c) FoIA: (Freedom of Information Act)

The freedom of Information Act is a federal freedom of information law that requires the full or partial disclosure of previously unreleased information and documents controlled by the United states government upon request.

D) FERPA

The Family Educational Rights and Privacy Act is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student.

E) CFAA

The Computer Fraud and Abuse Act is a United states cybersecurity bill that was enacted in 1986 as an amendment to existing computer fraud law, which had been included in the Comprehensive Crime control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization.

F) COPAA

The Council of Parent Attorneys 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 families.

G) VPPA

The video Privacy Protection Act was a bill passed by the United states congress to prevent what it refers to as "wrongful disclosure of video tape rental or sale records."

H) HIPAA

Health Insurance Portability and Accountability Act was created primarily to modernize the flow of healthcare information, stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage.

I) GLBA

The Gramm-Leach-Bliley Act, also known as the Financial Services modernization Act of 1999. It created to enhance competition in the financial services industry by providi a prudential framework for the affiliation of banks, securities firms, and other financial service providers, and for other purposes.

J) PCI DSS

The Payment card Industry Dates security standard is an information security standard for organizations that handle branded credit cards from the major card schemes.

K) FCRA

The Fair credit Reporting Act, Locs intended to protect Consumers from the willful and negligent inclusion of inaccurate information in their credit reports

L) FACTA

The Fair and Accurate credit Transactions Act to amend the Fair credit Reporting Act, to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer disputes

improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes.