Name - Ashwin Pandey Roll No :- 23

Page No:
Date:

Assignment - 1

Q-1) List of all symmetric algorithm.

→ Symmetric encryption is a type of encryption where one key is used to both encrypt and decrypt electronic information.

→ This encryption method differs from asymmetric encryption where a pair of keys, one public and one private is used to encrypt and decrypt message.

→ By using symmetric encryption algorithm data is converted to a form that can't be understood by anyone who does not passes secret key to decrypt it.

→ The secret key that the sender and recipient both use could be a specific password/code - or it can be random string of letter that have been generated by secure random number generator.

→ Type of symmetric encryption algorithm

1) Block Algorithm :-
Set length of bits - are encrypted in block of electronic data with the use of a specific key

2) Stream Algorithm :-
Data is encrypted as it stream instead of being retained algorithm include.

-> AES (Advanced encryption Standard)

-> DES (Data encryption Standard)

-> IDEA (International Data encryption algorithm)

-> Blowfish (Replacement for DES or IDEA)

-> RC4 (Rivest Cipher 4)

Q-2] List all assymetric key algorithm

-> Assymetric key algorithm work in a similar manner to symmetric key algorithm, where plain text is combined with a key, input to an algorithm and output cipher text

-> The key pair is comprised of a private key and a public key as the name imply, the public key is made available to everyone, where the private key is kept secret.

-> The two main uses of assymetric key algorithm are public key encryption and digital Signature. Public-key encryption is a method where anyone can send an encrypted message over a trusted network only receiver can decrypt message using the own private key.

-> Types of assymetric key algorithm

1) Diffie - Hellman key agreement

2) Rivest Shamir Adleman

3) Elliptic curve cryptography (ECC)

4) Digital Signature Algorithm (DSA)

Q-3] List the Algorithm for message digest.

-> Message digest algorithm refers to cryptographic hash functions to generate a unique value that is computed from data and a unique symmetric key.

-> A cryptographic hash function inputs data of various length and produces a unique value of all fixed lengths.

-> Adding a unique Symmetric key that shared between sender are required in order to compute message unique provides confidentiality so that the message cannot be easily changed if the text changed in an unauthorized or ~~manner~~ other manner.

-) List of message digest algorithm

1) Message Digest 5 (MD5)

2) Secure Hash Algorithm (SHA-1)

3) SHA 2 - 224

4) SHA 2 - 256

5) SHA 2 - 512

Assignment - 2

1) PII (Personally Indentifiable Information)

-> Phase-locked loop
-> A phase-locked loop or phase lock loop is a control system that generates an output signal whose phase is related to the phase of input signal.

2) The US privacy Act of 1974

-> The privacy act of 1974, established that governs a code of fair information practices that governs the collection, maintenance, use and dissemination of information about individuals that is maintained in system of record by federal agencies.

3) FOIA

-> Freedom of Information Act.
-> This provides public access to all federal agency records except for those record that are protected from disclosure by any of nine exemptions or three exclusions.

4) FERPA

-> The family Educational Rights & Privacy Act of 1974
-> This is united states federal law that governs the access to educational information and record

by public entities such as potential employees, public fund educational institution and foreign goverment.

5) CFAA

-> The Computer fraud and Abuse Act
-> It is United States Cyber security bill that was enacted in 1986 as an amendment to existing computer fraud law, which has been included in comprehensive crime control Act of 1984. The law prohibits accessing computer without authorization or in access authorization

6) CoPPA

-> Children's Online privacy protection Act
-> Congress enacted the action in 1998, COPPA required the federal trade commission to issue and enforce regulation concerning childrens online privacy.

7) VPPA

-> Video Privacy Protection Act.
-> It was passed by us congress in 1988. It was created to prevent what it refer to as "wrongful disclosure" video tyre rental or sale record or similar audio visual material to cover items such as video games and the future DVD format

8) HIPAA

-> Health Insurance Portability and Accountability Act of 1996
-> This is a federal law that required the creation of national standard to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

9) GLBA

-> German Leach Bliley Act
-> It is also known as the Financial modernization Act of 1999. It is united states federal law that requires financial institutions to explain how they share & protect their customer's private information.

10) PCI DSS

-> Payment Card Industry Data Security Standard
-> It is an information security standard for organization that handles branded credit cards from the major card-brand. The PCI Standard is mandated by the card brands but administrated by the payment card industry security Standard Council.

11) FCPA

-) Fair credit Reporting Act
-) This is a federal law the regulates the collection of consumer's credit information and access to their credit reports. It was passed in 1970 to address the fairness, accuracy and privacy of the personal information contained in the personal files of the credit reporting agencies.

12) FACTA

-) Fair and Accurate Credit Transactions Act
-) This is an amendment to that was added primarily to protect consumers from identity theft. The Act stipulates requirement for information privacy, accuracy and disposal and limits the ways consumer information can be shared.