ION:

Assignment - 7

7. List of all Symmetric Key Algorithms.

=>> Symmetric key encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information.

- The entities communicating via Symmetric encryption must exchang the key so that so that it can be used in the decryption process. this encryption method differs from asymetric 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 algorithm can not be understood by anyone who does not possess the secret key to decrypt it.

Two types of Symmetric Encryption

1. Block algorithms :-> Set lengths of bits are encrypted in blocks of electronic data with 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.

a). AES :- Advanced Encryption Standard

:-> The most Commonly used Symmetric algorithm is the AES, which was Originally known as Rijndael algorithm

:- this Standard Supersedes DES, which had been in use a block size of 128 bits, but can have threee different key lengths as shown with AES-128, AES-192. and AES-256

:- AES is very fast and Very Secure. Because of this, it's global uptake has been very quick.

b) DES :- Data Encryption Standard

— DES was originally devlopad in 1976. It has been one of the most widely used encryption algorithms.

:- The DES algorithms itself is very Strong. The weakness Comes in the fact that the Original DES Standard uses a 56-bit encryption key.

:- Basically, you Can use a Computer to run through all bit Combinations of the 56 key (1s and 0s) until you hit the right key.

:- It might take a day or so to run through all the Combinations. This is main Reason to DES is No longer widely used.

c) 3DES :- It is most Commonly known as Triple DES. 3DES gets its name because it applies the DES algorithm three time to each block of data.

- It able to use longer key lengths.
- A key must be specified for each of the 3DES encryption iterations. You have the Option of using the same key for each, same for two or Or different key for each iteration.

- most secure implementation is to use a different key for each iteration.

- If use same key for all three iteration, the key strength is considered to be 56 bits basically same as DES.

d) IDEA :- International Data Encryption Algorithm

- IDEA was Originally meant to be a replacement for the DES standard.

- IDEA uses a 128-bit encryption key.
- The first is the fact that IDEA is subject to a Range of Weak keys. The second reason is that there are Currently faster algorithms that Produce the same level of Security.

Eg RC4 :- It is fourth version of the Rivest Cipher. This key can vary from 40 to 256 bits.
- It is most commonly used 128 bits.

- RC4 is used in WEP and WPA on wireless network.

- It is also used in Secure Sockets Layer (SSL) and Transport Layer Security (TLS) with the Hypertext Transfer Protocol over SSL (HTTPS) Protocol.

Eg RC5 :- It is fifth version of Rivest Cipher.
- RC5 uses variable length encryption keys.
- Range. 2040 bits., Suggested key size : 128 bits

- At a one point, RSA, which owns the patent for RC5, was so sure of its security that it had a bounty system to reward anyone who could break itms encrypted with the algorithms.

2 List of all Asymmetric key Algorithms

=> Asymmetric encryption is also referred to as public key encryption.

- In Asymmetric encryption, Both the encrypting and decrypting systems have a set of keys.
- One is called the public key and another is Private key
- If the message is encrypted with One key in the pair, the message can be decrypted only with the other key in the Pair.
- Asymmetric Algo. used for encrypting or digitally signing data

eg. ① Diffie-Hellman :-> Diffie-Hellman key agreement algorithm was developed by Dr. Whitfield Diffie and Dr. Martin Hellman in 1976.

- Diffie-Hellman algo. is not for encryption or decryption but it enable two parties who are involved in Communication to generate a shared Secret key for exchanging information Confidentially.

b) Rivest Shamir Adleman (RSA) :-)

- Ron Rivest, Adi Shamir, Len Adleman released the Rivest-Shamir-Adleman (RSA) Public key algorithm in 1978.

- This algorithm can be used for encrypting and signing data. the encryption and signing processes are performed through a series of modular multiplications.

* Explaination

1. Ciphertext = (plaintext)^e mod n
2. plaintext = (Ciphertext)^d mod n
3. Private key = {d, n}
4. Public key = {e, n}

c) EL Gamal :- EL Gamal is an algorithm used for transmitting digital signatures and key exchanges. The method is based On Calculating logarithms. EL Gamal algorithm is based On the characteristics of logarithmic numbers and calculations. The digital Signature algorithm (DSA) is based on EL Gamal algo.

d) Elliptic Curve Cryptography (ECC):- Elliptic Curve Cryptography provides similar functionality to RSA. Elliptic Curve Cryptography is being implemented in ~~sim~~ smaller devices like cell phones. it requires less Computing power Compared with RSA. ECC encryption Systems are based On the idea of using points On a Curve to define the public/private key pair.

e) Digital Signature Algorithm (DSA): the DSA was developed by the U.S. government for digital signatures DSA can be used Only for signing data and it can not be used for encryption.

- The DSA Signing process is performed through a series of Calculations based On a Selected prime number, A

- Although intended to have a maximum key size of 1024 bits.

- the process of creating the digital signature is faster than validating it.

Que: 3 List the Algorithms for message digest.

=> Message digest algorithms rely on 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 arbitrary length and produces a unique value of a fixed length. Because message digest algo. generate a value that is always used in encrypted form, they are sometimes known as encryption-only algorithm".

2) Adding a unique Symmetric key that is shared between a Sender & Receiver in order to compute a message digest value provides Confidentiality to ensure that the message digest cannot be easily changed if the data is changed in an unauthorized or other unexpected manner.

* List of message digest algo.
1. Message Digest 5 (MD5)
2) Secure Hash Algo. (SHA-1)
3) SHA2-224
4) SHA2-256
5) SHA2-512

★ PII (Personally Identifiable Information)

- PII is data which can be used to identify, locate or contact an individual and includes information like name, date of birth, place of residence, credit card information, phone number, race, gender, criminal record, age and medical records.

b ★ US Privacy Act of 1974 :-»

- 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

FOIA provides public access to all federal agency records except for those records (or portions of those records) that are protected from disclosure by any of nine exemptions or three exclusions.

d. FERPA - Family Educational Rights and Privacy Act :-) is a federal law enacted in 1974 that protects the privacy of student education records.

E. CFAA :-> Computer Fraud and Abuse Act.
- CFAA was enacted in 1986, as an amendment to the first federal Computer Fraud law to address hacking.

F. COPAA :-> Computer Operator and Programming Assistant.

G. VPAA :- Video Privacy Protection Act.
VPPA :- Virtual Power Purchase Agreement
:- VPPA is basically a form of Price hedge. the Project pays the Company if the electricity is sold into the market above the agreed Contract Price and the Company pays the Project the diff. if the electricity falls below the agreed price.

H. HIPAA :-> Health Insurance Portability and Accountability Act of 1996.

- HIPAA is a federal law that required the Creation of National Standards to Protect Sensitive Patient Health information from being disclosed without the patient's Consent or Knowledge.

J. GLBA :-> Gramm-Leach-Bliley Act also known as Financial Modernization Act of 1999.

In this law requires financial Institutions to explain how they Share and Protect their Customers's private Information.

I: PCI DSS :- Payment Card Industry Data Security Standard.

:) PCI DSS is a set of requirements intended to ensure that all Companies that Process, Store or transmit Credit Card Information maintain a Secure Environment

K. FCRA :- Foreign Contribution Regulation Act, 1976 Casts Certain Obligation on banks in regard to acceptance of foreign inward remittances for Onward Credit to the Accounts of associations / Organisations in Indi

FATCA

L. FACTA :-> Foreign Account Tax Compliance Act
Fair and Accurate Credit Transactions Act

:. the Purpose of the FACTA is to Prevent identity theft, improve resolution of Consumer disputes, improve the accuracy of Consumer records, and make improvements in the use of and Consumer Access to Credit Information