Name = Ronak Parmar
Roll NO - 25

Assignment - 1

(1) List all Symmetric key algorithms.

→

(1) AES (Advanced Encryption Standard) : AES is a most commonly used symmetric algorithm. which was originally known as Rijndael. Used for the encryption of electronic data. This standard supersedes DES.

(2) DES (Data Encryption Standard) : In "Modern" Computing, DES was the first standardized cipher for securing electronic communication and used in variations.

(3) IDEA (International Data Encryption Algorithm) : This is replacement for the DES standard. IDEA uses a 128-bit encryption key. Currently IDEA is not widely used because there are currently faster algorithm that produce the same level of security.

(4) RC4 : This is a fourth version of the Rivest Cipher. Uses a variable length encryption key. It's most commonly used with a 128 Bit key. This is very simple & easy to implement. Used in WEP and WPA on Wireless network.

(5) RC5 : This is fifth version of Rivest Cipher. Uses a variable length encryption keys. Range up to 2040 Bits. Suggested size is 128 Bits. RSA, owns the Patent of RC5, was so sure that it had a Bounty system to reward who Break items encryption with the algorithm.

② List all asymmetric key algorithms.

→

① RSA (Ron Rivest, Adi Shamir, Adleman) : Mostly widely used asymmetric encryption algorithm. Its potency lies in the "Prime factorization" method that it relies upon. Basically this method involves two huge random Prime numbers and these numbers are multiplied to create another giant number. A great Advantage is its scalability. used in SSL, Crypto currencies and email encryption.

② ECC (Elliptic Curve Cryptography) : Like RSA, ECC also works on the Principle of irreversibility means easy to compute it in one direction but painfully difficult to reverse it and come to the Original Point. In ECC a number symbolizing a Point on the curve is multiplied by another number and gives another Point on the Curve. Uses in Smaller devices like Cell Phone.

③ Diffie Hellman

③ List the algorithm for message digest

→

① MD5 : MD5 takes an input of any size and Produces an output if a 128 Bit hash value. It is impossible to generate a message having the same hash value.

② SHA : These algorithms have been Compromise with collision Resistance attacks. This require collision-Resistance Properties such as Password storage and time stamp generating. SHA-1 is used for hashing Password..

Name : Ronak Parmar
Roll No : 25

Assignment-2

(1) PII : Personally identifiable information is information that, when used alone or with other relevant data, can identify an individual.

(2) US Privacy Act of 1974 : Establishes a Code of fair information Practices that governs the collection, maintenance, use and dissemination of info. that about individuals that is maintained in system.

(3) FOIA : Freedom of information Act is a federal law that requires the full or partial disclosure of previously unreleased information and documents controlled by the US upon request.

(4) FERPA : Family Educational Rights and Privacy act is a federal law that protects the Privacy of student education record.

(5) CFAA (Computer Fraud & Abuse Act) : The Law Prohibits accessing a Computer without authorization or in excess of authorization.

(6) COPPA : (Childsen's online Privacy Protection act) : Law is created to protect the Privacy of Childsen under 13. and sites require Parent Consent for Collection & information of Young users.

(7) VPPA (Video Privacy Protection act) : Strongest Protection of Consumer Privacy against a specific form of data Collection. It Prevent disclosure of Personally identifiable information and visual material.

(8) HIPAA (Health Insurance Portability and Accountability Act) : The law is for medical Records and for ~~Fraud~~ address limitation healthcare insurance Coverage.

(9) GLBA (Gramm-Leach-Bliley act) : law the required financial institution to explain how they Protect Private information.

(10) FCRA : (Foreign Contribution (Regulation) act : law is for Regulate the acceptance of foreign Contribution.

(11) FACTA : (fair and accurate Credit transaction act) : Protect Consumer from identity theft.

(12) PCI DSS : Payment Card Industry data Security Standard : for organisation that handle Branded Credit Card from the major card Schemes.