NANDAKRISHNAN NAIR
Roll no 22
MCA Sem 1
HARDIK JOSHI SIR

Date 18th Jan 2021

ASSIGNMENT 1

Symmetric key Algorithms are as follows:-

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES/IDEA
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)
- 3DES OR TDEA (Triple data encryption Algorithm)

Asymmetric key Algorithm are as follows:-

- Ed25519 Signing
- X25519 key exchange
- Ed448 signing
- X448 key exchange
- Elliptic Curve Cryptography
- RSA (Rivest Shamir Adleman)
- DSA (Digital Signature Algorithm)
- Diffie-Hellman key exchange
- key serialization

Page No.
Date

Message Digest Algorithms are as follows:-

~~SHA2 2~~ SHA2 - family (Secure Hash Algorithm)

- SHA2 - 224
- SHA2 - 256
- SHA 2 - 384
- SHA 2 - 512
- MD 2 (Message Digest 2)
- MD 5 (Message Digest 5)
- SHA - 0
- SHA - 1
- SHA 3 - 224
- SHA 3 - 256
- SHA 3 - 384
- SHA 3 - 512

Page No.
Date

NANDAKRISHNAN NAIR
ROLL - 22
MCA Sem 1
HARDIK JOSHI SIR

Date 18th JAN 2021

ASSIGNMENT 2

a) PII (Personally Identifiable Information)

- PII is any data that can be potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used to deanonymizing previously anonymous data.

b) US Privacy Act of 1974

- The Privacy act of 1974 established 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 is a law that requires the full or partial disclosure of previously unreleased information and documents controlled by US

government upon request. The act defines agency records subject to disclosure and defines nine exemptions to the salute

d) FERPA (Family Educational Rights and Privacy Act)

- FERPA gives parents access to their educational ~~rights~~ records, an opportunity to seek to have records ammended, and some control over the disclosure of information
- With several exceptions, schools must have a students prior consent to disclosure of records.

e) CFAA (Computer fraud and Abuse Act)

- CFAA is an amendment to existing computer fraud law. The law prohibits accessing a computer without authorization, or in excess of authorization.

f) COPAA (Council of Parent Attorneys and Advocates)

- COPAA is an independent national American association of parents of children with disabilities, advocates

and related professionals who protect the legal and civil rights of student with disabilities and their parents

g) VPPA (Virtual Power Purchase Agreement)

- within VPPA contract the corporate buyer does not own & is 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)

- HIPAA is a federal law that required the creation of national standards 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 institutions to explain how they share and protect their customer's private information.

- financial companies must communicate to their customers how they share their customers sensitive data.

j) PCI DSS (Payment Card Industry Data Security Standard)

- It is a standard for organizations that handle branded 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)

- FCRA is a federal law that regulates the collection of consumers credit information and access to their credit reports.
- Used to address the fairness accuracy and privacy of the personal information.

l) FACTA (Fair and Accurate Credit transactions Act)

FACTA is an amendment to FCRA that was ended, primarily to protect consumers from identity

theft. The Act stipulates requirements for information privacy, accuracy and disposal and limits the ways consumers information can be shared.