Page No.:
Date:

Name: Azbaaz Shaikh
Batch: MCA I 2020-21
Subject: IoM Assignment 2

Q1) List all symmetric key algorithms:

A) (i) AES (Advanced Encryption Standard)
(ii) DES (Data Encryption Standard)
(iii) IDEA (International Data Encryption Algorithm)
(iv) Blowfish (Drop-in replacement for DES & IDEA).
(v) RC4 (Rivest Cipher 4)
(vi) RC5 (" " 5)
(vii) RC6 (" " 6)

Q2) List all asymmetric key algorithms:

A) (i) Ed 25519 signing
(ii) X25519 key exchange
(iii) Ed448 signing
(iv) X448 key exchange.
(v) Elliptic curve cryptography.
(vi) RSA.
(vii) Diffie-Hellman key exchange.
(viii) DSA
(ix) Key serialization.
(x) Asymmetric Ratchets.

Page No.:
Date:

Q3) List all algorithms for message digest.

A) (i) SHA3-512
(ii) SHA-384
(5) SHA
(iv) SHA3-384
(7) SHA-224
(6) SHA-512/256
(8) SHA-256
(8) MD2
(9) SHA-512/224
(10) SHA3-256
(11) SHA-512
(12) MD5
(13) SHA3-224.

* Discuss Briefly.

(a) PII (Personally Identifiable Information)

→ Personally Identifiable Information is any data that could potentially identify a specific individual - Any information that can be used to distinguish one person from another person and can be used to deanonymize previous anonymous data.

(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 record by federal agencies.

(c) FOIA.

→ The FOIA provides public access to all federal agencies records except for those records that are protected from disclosure by any of nine exemptions or three exclusions.

Page No.:
Date:

d) FERPA

→ FERPA is a federal law enacted in 1974 that protects the privacy of student education records.

e) CFAA

→ The CFAA is a US cybersecurity bill enacted in 1986 as an amendment to existing computer fraud law.

f) COPAA

→ The COPAA is an independent national American association of parents of children with disability, attorneys, advocates & professionals with legal rights to protect the children with disabilities & their families.

(g) VPPA

→ A VPPA is a purely financial contract that provides RECs from a specific renewable energy project located off your company's property.

(h) HIPAA

→ The HIPAA of 1996 is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without patient consent.

(i) GLBA

→ The GLBA requires financial institutions to explain their information-sharing practices to their customers & to safeguard their data.

(j) PCI DSS

→ PCI DSS is a set of requirements intended to ensure that all companies that store process, or transmit credit card information maintain a secure environment.