Assignment 1

1] List of all symmetric algorithms.

→ Symmetric 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 exchange the key so that it can be used in the dey decryption process.

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

→ There are two types of symmetric encryption algorithms :

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

- 2) Stream algorithms :-
  Data is encrypted as it stream instead of being retained in the system's memory.

→ Some examples of symmetric encryption algorithms include :

- 1.) AES (Advanced Encryption Standard) :-
  The most commonly used symmetric algorithm is the Advanced Encryption Standard (AES), which was originally known

as Rijndeal. This is the standard set by the U.S. National Institute of Standards and Technology in 2001 for the encryption of electronic data announced in U.S. FIPS PUB 197.

The AES cipher has a block size of 128 bits, but can have three different key key lengths as shown with AES-128, AES-192 and AES-256.

– 2) DES (Data Encryption Standard) :-

In "modern" computing DES was the first standardized for securing electronic communications, and is used in variations. The original DES is not used anymore as it is considered too "weak", due to the processing power of modern computers.

Even 3DES is not recommended by NIST and PCI DSS 3.2, just like all 64-bit ciphers.

– 3) IDEA (International Data Encryption Algorithm) :-

In cryptography, block cyphers are very important in the designing of many cryptographic algorithms and are widely used to encrypt the bulk of data in chunks. By chunks, it means that the cypher takes a fixed size of the plaintext in the encryption process and generates a fixed size chip ciphertext using a fixed-length key. An algorithm's strength is determined by its key length.

4) Blowfish :-

Blowfish is a symmetric block cipher. It uses a variable-length key ranging from 32 to 448 bits. Blowfish was designed in 1993 by Bruce Schneier. It has been analyzed extensively by the cryptography community and has gained wide acceptance. It is also a noncommercial product, thus making it attractive to budget conscious organizations.

5) RC4 (Rivest cipher 4) :-

All the other symmetric algorithms we have discussed have been blocks ciphers. RC4 is a stream cipher developed by Ron Rivest, RC is an acronym for Ron's cipher, or sometimes Rivest's cipher There are other RC versions, such as RC5 and RC6.

2) List all asymmetric key algorithms.

→ There are two sides in an encrypted communication : the sender, who encrypts the data, and the Recipient, who decrypts it.

- As the name implies, asymmetric encryption is different on each side ; the sender and the recipient use two different keys.

- Asymmetric encryption, also known as Public key encryption, uses a Public key - Private key Pairing : data encrypted with the private key can only be decrypted with the public key and vice versa.

- TLS the Protocol the makes HTTPS possibl relies on asymmetric encryption : A client will obtain a bebsite's Public key from that website's TLS certificate and uses that to initiate secure communication. The website keeps the private key secret.

→ The following are the major asymmetric encryption algorithms :-

- 1) Diffie - Hellman key agreement :-

Diffie - Hellman key agreement algorithm was developed by Dr. Whitfield Diffie and Dr. Martin Hellman in 1976. Diffie - Hullman algorithm is not for encryption or decryption but it enable two parties who are involved in key agreement can be explained communication to generate a shared secret key for exchanging information confidentially.

2) Rivest Shamir Adleman (RSA) :-

Ron Rivest, Adi Shamir, and Len Adleman released the Rivest-Shamir-Adleman (RSA) Public key algorithm in 1978. This algorithm can be used for encryption and sin signing data. The encryption and signing processes are performed through a series of modular multiplications.

3) Elliptic curve cryptography (ECC) :-

Elliptic curve cryptography provides similar functionality to RSA. Elliptic curve cryptography is being implemented in smaller devices like cell phones.

It requires less computing power compared with RSA. ECC encryption system are based on the idea of using points on a curve to define the public / private key pair.

4) Digital signature Algorithm (DSA) :-

The Digital signature Algorithm was developed by the united states government for digital signatures. Digital signature Algorithm can be used only for signing data and it cannot be used for encryption.

The DSA signing process is performed through a series of calculations based on a selected prime number. Although intended to have a maximum key size of 1,024 bits, longer key sizes are now supported.

when DSA is used the process of creating the digital signature is faster than validating it.

3) List the algorithms for massage 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 cryptography hash function inputs data of arbitrary length and produces a unique value of a fixed length. Because message digest algorithms generate a value that is always used in encrypted from, they are sometimes know as encryption-only algorithms.

- Adding a unique symmetric key that is shared between a sender and receiver in order to computer message digest value, provides confidentiality to ensure that the if the data is changed in an unauthorized or other manner.

→ The following are the message digest algorithms :-

- 1] Message digest 5 (MD5) :-

The MD5 hashing algorithm is a one-way cryptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.

The MD5 hash function was originally designed for use as a secure cryptography hash algorithm for authentication digital signatures.

MD5 has been deprecated for uses other than as non-cryptographic checksum to verify data integrity and detect unintentional data corruption.

Although originally designed as a cryptographic message authentication code algorithm for use on the internet, MD5 hashing is no longer considered reliable for use as a cryptographic checksum because researchers have demonstrated ~~tea~~ techniques capable of easily generating MD5 collisions on commercial off-the-shelf computers.

2) Secure Hash Algorithm (SHA-1) :-

The secure Hash Algorithm are a family of cryptographic hus functions published by the National Institute of standards and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS)

A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National security Agency (NSA) to be part of the Digital signature Algorithm.

cryptographic weaknesses were discovered in SHA-1 and the standard was no longer approved for most cryptographic uses after 2010.

3) Elliptic curve cryptography (ECC) :-

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over Finite Fields.

ECC allows smaller keys compared to non-EC cryptography to provide equivalent security.

Elliptic curves are applicable for key agreement digital signatures, Pseudo-random generators and other tasks. Indirectly, they ca be used for encryption by combining the key agreement with a symmetric encryption scheme.

They are ets also used on several inte Factorization algorithms based on elliptic cur that have applications in cryptography, suc as lenstra elliptic-curve Factorization.

4] Digital signature Algorithm (DSA) :-

The Digital signature Algorithm is a Federal information processing standard for digital signature, based on the mathematical concept of modular exponentiation and the discrete logarithm problem. DSA is a variant of the Schnorr and ElGamal signature schemes.

The National Institute of standard an Technology (NIST) proposed DSA for use in their Digital signature standard (DSS) in 1991, and adopted is as FIPS 186 in 1994.

A draft version of the specification FIPS 186-5 indicates DSA will no longer be approved for digital signature generation but may be used to verify signature generated prior to the implementation date of that standard.

1] Discuss briefly one-two sentences

a] PII (personally In Identifible Information)

-> PII is often referenced by us government agencies and non-governmental organizations yet the us lacks one overriding law about PII. so your understanding of PII may differ depending on your particular situation.

The most common definition is provided by the National Institute of standards and Technology (NIST).

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 in systems of records by federal agencies.

c] FOIA

-> Since 1967, the Freedom of information Act (FOIA) has provided the public the right to request access to records from any federal agency. It is often described as the law that keeps citizens in the know about their government.

d] FERPA

-> FERPA (Family Educational Rights and privacy Act of 1974) is legislation that protects the privacy of students personally identifiable information (PII). The act applies to educational institution that receive federal funds.

e] CFAA

→ The computer fraud and abuse Act (CFAA) of 1986 is united stage legislation that made it a federal crime to access a protected computer without proper authorization.

F] COPPA

→ The children's online privacy protection Act (COPPA) is a law passed by the U.S. Congress in 1998 to specifically protect the privacy of children under the age of 13 by requesting ~~Rem~~ parental consent for the collection of use of any personal information of website users. The Act officially took effect in April 2000. COPPA is managed by the federal trade commission (FTC).

g] VPPA

→ A virtual power purchase Agreement (NPPA) also known as a synthetic PPA or contract for Differences is a popular type or renewable energy contracting structure that provides a financial hedge against future energy fluctuations.

h] HIPAA

→ The 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.

i] GLBA

→ The Gramm-Leach-Bliley Act (GLBA is also known as the Financial modernization Act of 1999. it is a united states Federal law that requires Financial institutions to explain how they share and protect their customers private information.

j] PCI DSS

→ The Payment card industry Data security standard (PCI DSS) is a set of security standards formed in 2004 by visa, Mastercard Discover Financial services, JCB international and American express.

Governed by the payment card industry security standards council (PCI SSC), the compliance scheme aims to secure credit and debit card transaction against data theft and fraud.

k] FCRA

→ The Fair credit Reporting Act (FCRA) is a Federal law that ~~re~~ 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 files of the credit reporting agencies.

L] FACTA

→ FACTA (Fair and Accurate credit transactions Act) is an amendment to FCRA (Fair credit Reporting Act) that was added, primarily, to protect consumers from identify theft. The act stipulates requirements for information privacy, accuracy and dissposal and limits the ways consumer information can be shared.