ame : Rathod Ami K.

Roll No : [redacted] 33

Assignment -1 , Q

1 List ~~of~~ all symmetric key algorithms

→ There are two types of symmetric encryprition algorithms

1) Block algorithms:-

→ Set lenghts of bits are encrypted in blocks of electronic data with the use of a specific secret key. As data is being encrypted, the system holds tha data in its memory as it waits for complete blocks.

2) Stream algorithms:-

→ Data is encrypted as it Streams instred of being retained in system's memory

→ Example

→ AES (Advanced Encryption Standard)

→ DES (Data Encryption Standard)

→ IDEA (International Data Encryption Algoritum)

-> Blow fish (Drop-in replacement for DES or IDEA)

-> RC4 (Rivest cipher 4)

-> RC5 (Rivest cipher 5)

-> RC6 (Rivest cipher 6)

2 List all asmmetric key Algorithms

→ ~~a~~ Asymmetric cryptography is branch of cryptography where a secret key can be devided in two part..

→ Ed25519 signing

→ X25519 key

→ Ed448 signing.

→ X448 key exchange

→ RSA

→ Dffie - Hellman key exchange.

→ DSA

→ key serialization.

→

(3) List the algorithms for message digest

→ Messege digest algorithms is a widely used hash function producing a 128-bit hash value

→ list of message digest algorithms

→ MD2 ⇒ The MD2 messege digest Algorithm as Define in RFC 1319

→ MD5 →. The MD5 message digest Algorithm as difine in RFC 1321

→ SHA-1, SHA-224, SHA-256, SHA-384, SHA.1224, SHA 6121256

→ SHA 3-224, SHA 3-256, SHA 3-284 SHA 3-512