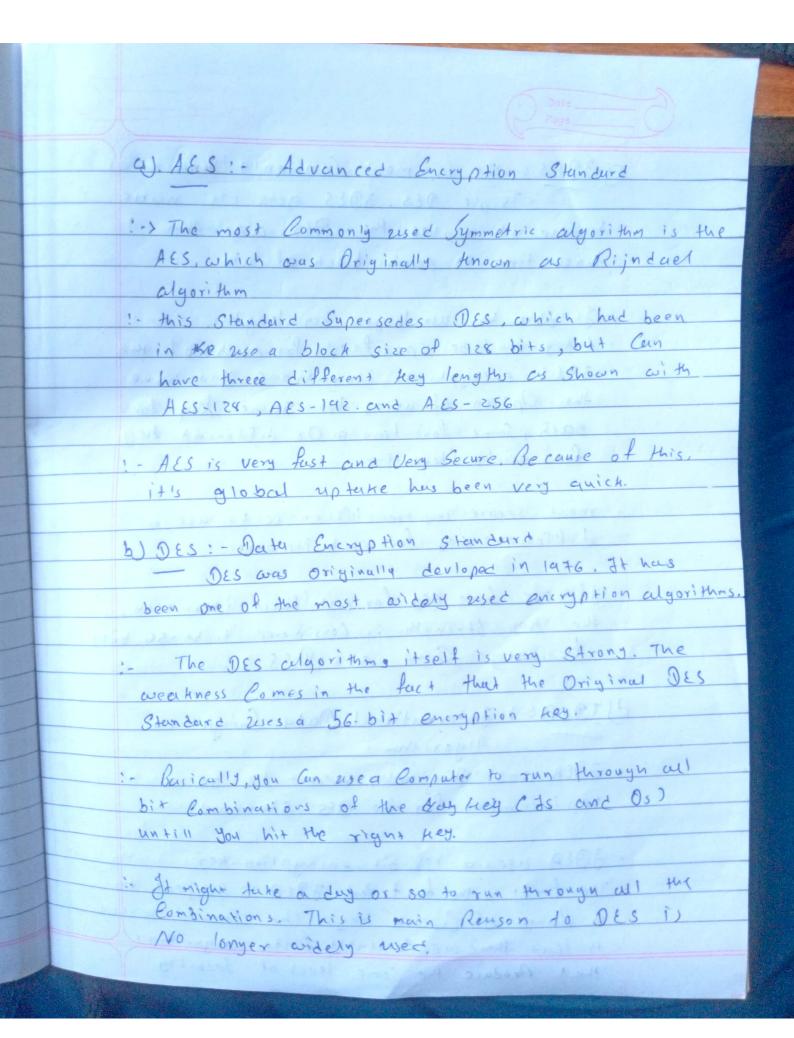
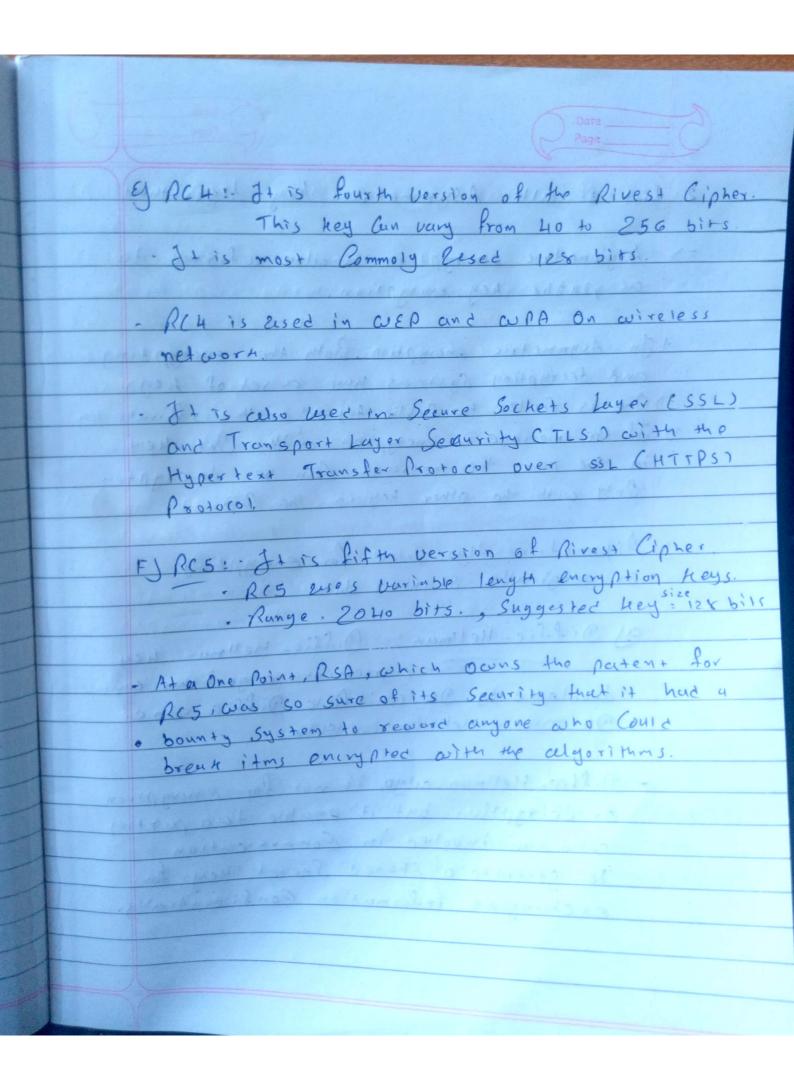
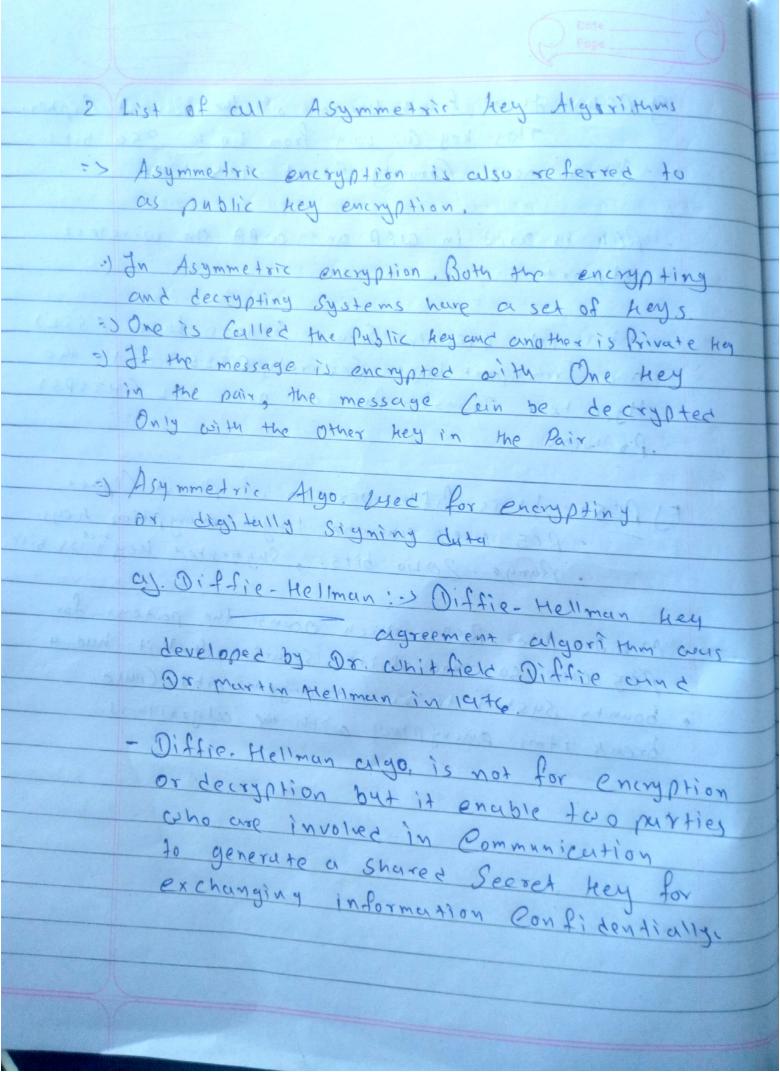
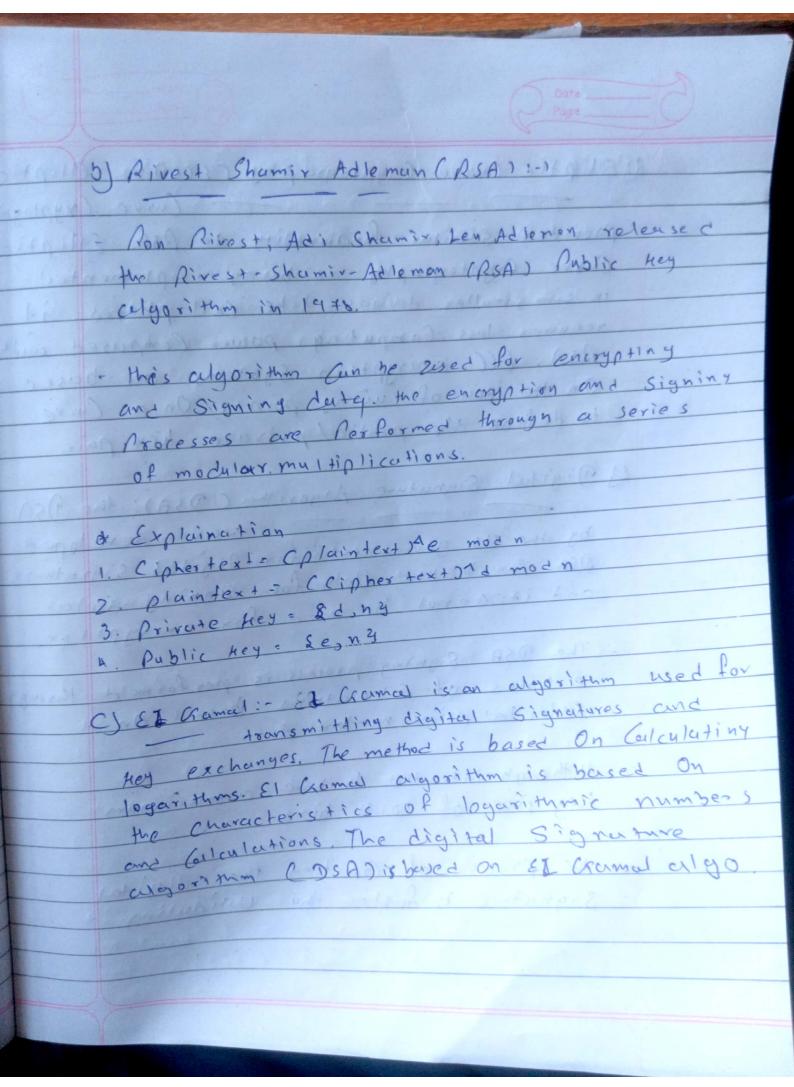
ION: Assignment - J J. List of all Symmetric key Algorithms =>> Symmetric key encryption is a type of encryption where Only one key (a Secret key) is rised to both encrypt and decrypt electronic information. The entities Communicating via Symmetric encryption must exchang the key so that so that it can be essed in the decryption process this encryption method differs from asymetric encyption where a pair of keys, One Public and one Private, is used to encrypt and decrypt By rising symmetric encryption algorithms data is Converted to a form that edgery to Cun not be understood by anyone who does not possess the Secret key to decrypt it. # Too types of Symmetric Encryption is. Block algorithms: >> Set lengths of bits are encrypted in blocks of electronic dute with use of a specific Secret key. As the deita is being energy ted the System holds the darta in its memory as it waits for Complete Blocks.



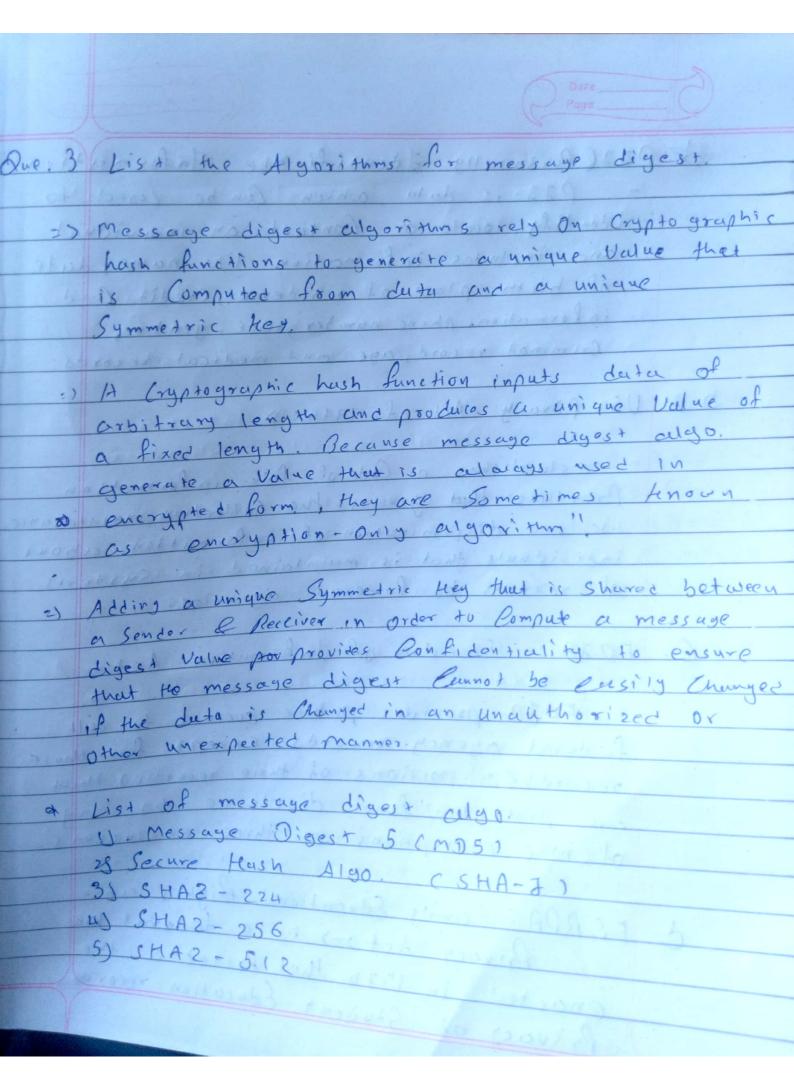
C1:3DES: It is most Commonly known as Triple DES. 3DES gets its name because it applies the DES algorithm three time to euch block of duty. - It able to uso longer key lengths. - A key must be specified for each of the 3DES encryption iterations. You have the Option of using the same key for each, Same for two or Or different key for each iteration most secure implementation is to use a different key for ouch iteration S. SEPT MA MORALUSK ALLENGED 2000 230 T - It use same key for can three iteration, the key Strength is Considered to be 56 bits basically Same as DES. the trade of the trade of the sail of the ditDEA: ) International Data Encryption Algorithm - JOEA was Originally mount to be a replacement for the DES steindard. and water all the day working - JDEA uses a 12x. bit emeryption key. - The first is the fact that JDEA is Subject to a Range of Wenk Keys. The Second senson is that there are Currently faster algorithms that Produce the Same level of Seenrity







di Elliptic Curve Cryptography CECCO:- Elliptic - Curve Coryptography Provides Similar functionality to RSA. Elliptic Curre Cryptography is being implemented in sim smaller devices like cell phones, it requires less Computing power Compared with 25A. Ell encryption Systems one based On the idea of using pointy On a Curve to define the public/private key pair. south and offered rolling & Digital Signature Algorithm (DSA): the DSA was developed by the U.S. government for digited signatures DSA Coun be used donly for signing duty and it connot be used for energht on . The DSA Signing process is performed through a series of Calculations based on 4 Selected prime number, A State of the water of the supported - Although intended to have a maximum key size of 1024 bits. Con Ex Applicable and To propose and will the process of creenting the digital Signature to Soster than Unliderling it



A PJJE Personally Jeensifiable Information - PJJ is data which Can be used to identify, locate or Contact an individual and includes information like name, date of birty place of residence, Credit Gird information, phone number, race, gender, Criminal record, age and medical records extends stages mailsoned died since applicate fine b & US Privacy Act of 1974:->> - 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 records by federal agencies. C. FOJA: Freedom of Information Act cases with tomother country to be to be a start took FOJA provides public cicess to cell federal agency records except for those records (or portions of those records) that are protected from disclosure by any of nine exemptions or three exclusions L'AMERICA COMPONENTAL d. FERPA- Family Educational Rights and Privacy Act 2-) is a federal law enacted in 1974 that Protects the Privacy of Student Education records

