

**Cryptography Assignment 3**

**B.Tech CSE**

**Submitted By: Samriddh Goyal**

**Submitted To: Ashutosh Sharma**

**Samriddh Goyal**

**V Semester, B-1 SapID:500086928**

**Roll No: R2142201757**

**1. Explain short notes on the following in detail:**

1. **Smart card security**: brilliant cards give approaches to safely recognize and validate the holder and outsiders who need admittance to the card. For instance, a cardholder can utilize a PIN code or biometric information for validation. They likewise give an approach to safely store information on the card and safeguard correspondences with encryption.
2. **Biometric Authentication:** Biometric validation is a security cycle that depends on the novel natural qualities of people to confirm they are who they say they are. Biometric verification frameworks contrast physical or social characteristics with put away, affirmed, true information in a data set.
3. **SSL and TLS:** SSL represents Secure Attachment Layer while TLS represents Transport Layer Security. Both Secure Attachment Layer and Transport Layer Security are the conventions used to give security between internet browsers and web servers. The principal contrast between Secure Attachment Layer and Transport Layer Security is that, in SSL (Secure Attachment Layer), the Message digest is utilized to make an expert mystery and it gives the essential security administrations which are Confirmation and classification. while In TLS (Transport Layer Security), a Pseudo-irregular capability is utilized to make an expert mystery.
4. **Database access control:** Data set admittance control, or DB access control, is a strategy for permitting admittance to an organization's delicate data just to client bunches who are permitted to access such information and confining admittance to unapproved people to forestall information breaks in data set frameworks.
5. **RFID and privacy issues in RFID:** The security issues and the specialized difficulties looked by the RFID labels in turning into a key innovation are examined. Two outstanding security issues incorporate spilling data relating to individual property, and following the buyer's spending history and examples and actual whereabouts

**2. Discuss zero-knowledge protocol in details:**

In cryptography, a zero-information evidence or zero-information convention is a strategy by which one party (the prover) can demonstrate to another party (the verifier) that a given assertion is valid while the prover tries not to pass on any extra data separated from the way that the assertion is to be sure obvious.

3**. Explain “Double DES and triple DES” with the help of block diagram.**

**DOUBLE DES:**

DOUBLE DES is an encryption procedure which utilizes two occasions of DES on same plain text. In the two cases it utilizes different keys to scramble the plain text. Both keys are expected at the hour of unscrambling. The 64-bit plain text goes into first DES case which then changed over into a 64-bit canter text utilizing the primary key and afterward it goes to second DES occasion which gives 64-bit figure text by utilizing second key.

**Triple DES:**

Triple DES is an encryption method which utilizes three cases of DES on same plain text. It involves their various kinds of key picking strategy in first undeniably utilized keys are unique and in second two keys are same and one is unique and in third all keys are same.