TERNA ENGINEERING COLLEGE, NERUL
Department of Computer Engineering

Cryptography and System Security (CSS)

Assignment No 3 (Beyond Syllabus To fill Curriculum Gap)

Sr. No	Question
Q. 1	Explain Internet Key Exchange
Q. 2	Describe Biometric performed using various techniques
Q. 3	Explain the concept of ZERO KNOWLEDGE

CSS ASSIGNMENT - 3

AMEY THAKUR

COMPS TE B-50

Amey

AMEY TE B 50 Amey

PAGE No.
DATE / /

Q.1 Explain Internet Key Exchange

Ans:

Internet Key Exchange (IKE)

- The Internet Key Exchange (IKE) is an IPSec (Internet Protocol Security) standard protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access.
- Specified in IETF Request for Comments (RFC) 2409, IKE defines an automatic means of negotiation and authentication for IPsec Security Associations (SA).
- Security Associations are security policies defined for communication between two or more entities; the relationship between entities is represented by a key. The IKE protocol ensures security for SA communication without the preconfiguration that would otherwise be required.
- A hybrid protocol, IKE implements two earlier security protocols, Oakley and SKEME, within an ISAKMP (Internet Security Association and Key Management Protocol) TCP/IP based framework.
- ISAKMP specifies the framework for key exchange and authentication, the oakley protocol specifies a sequence of a key exchanges and describes their services (such as identity protection and authentication). and SKEME specifies the actual method of key exchange.

AMEY TE B 50 Amey

- Although IKE is not required for IPSec configuration, it offers a number of benefits, including: automatic negotiation and authentication; anti - replay services; Certification Authority (CA) support; and the ability to change encryption keys during an IPSec session.

AMEY TE B 50 Amey

PAGE No.
DATE / /

Q.2 Describe Biometric performed using various techniques.

Ans:

- Biometrics is the measurement and statistical analysis of people's unique physical and behavioral characteristics. The technology is mainly used for identification and access control or for identifying indivisuals who are under surveillance.
- The basic premise of biometric authentication is that every person can be accurately identified by their intrinsic physical or behavioral traits. The term biometrics is derived from the Greek words bio, meaning life, and metric, meaning to measure.

How biometrics works.

- Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics and point-of-sale (POS) applications.
- In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry.
- Some biometrics methods, such as measuring a person's gait, can operate with no direct contact with the person being authenticated

AMEY TE B 50 Amey

PAGE NO.

DATE / /

Components of biometric devices includes:

- A reader or scanning device to record the biometric factor being authenticated.
- Software to convert the scanned biometric data into a standardized digital format and to compare match points of the observed data with stored data.
- A database to securely store biometric data for comparison.

- Biometric data may be held in a centralized database although modern biometric implementations often depend instead on gathering biometric data locally and then cryptographically hashing it so that authentication or identification can be accomplished without direct access to the biometric data itself.

Types of biometrics

1. Facial Recognition
2. Fingerprints
3. Finger Geometry (the size and position of fingers)
4. Iris Recognition
5. Vein Recognition
6. Retina scanning
7. Voice Recognition
8. DNA (deoxyribonucleic acid) matching
9. Digital Signatures.

AMEY TE_B 50 Amey

PAGE No.

DATE / /

Advantages of biometrics

- Hard to fake or steal, unlike passwords
- Easy and convenient to use
- Non-transferrable
- Efficient because templates take up less storage.
- Generally, the same over the course of user's life.

Disadvantages of biometrics

- It is costly, to get a biometric set up and running
- If the system fails to capture all the biometric data, it can lead to failure in identifying a user.
- Databases holding biometric data can still be hacked
- Errors such as false rejects and false accepts can still happen.

AMEY TE B 50 Amey

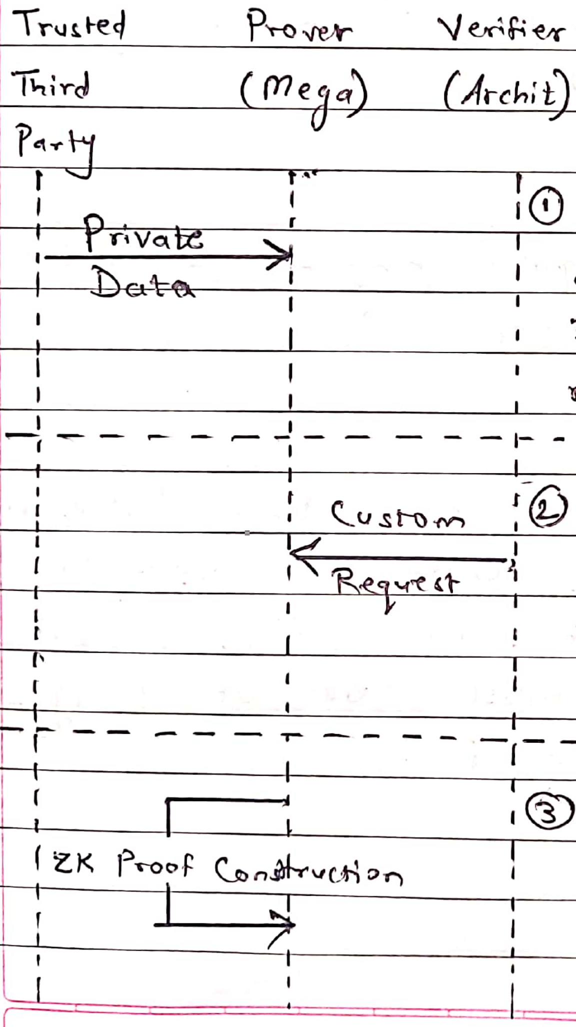
Q.3. Explain the concept of ZERO KNOWLEDGE

Ans:

Zero Knowledge Proof

- Zero Knowledge Proof is an encryption scheme proposed by MIT researchers Silvio micali Shaffi Goldwasser, and Charles Rackoff in the 1980s.
- In this method, one party (Proover) can prove that a specific statement is true to the other party (Verifier) without disclosing any additional information.

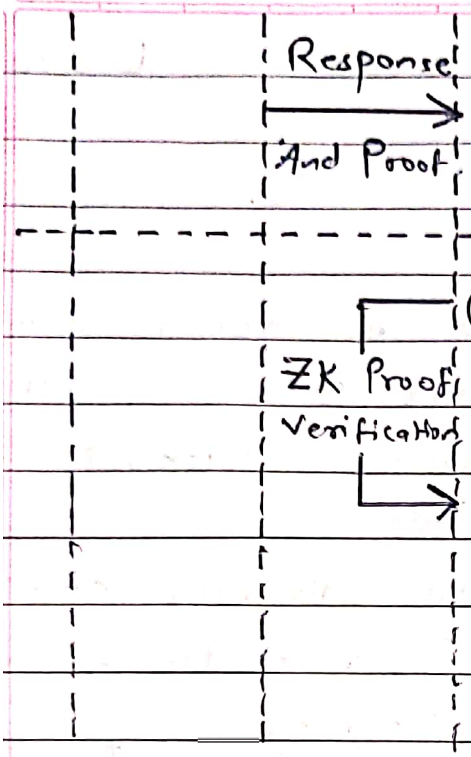
Zero Knowledge Protocol : Data Exchange



① The Prover gets some authenticated private data. eg. Signed bank statement. It could happen on demand or regularly, once per month, for instance.

② The verifier makes a custom request on Prover's personal data. The requests should ask for the necessary minimum

③ The prover computes the response on the verifier's question and constructs the proof of correct computation.



④ Both response and proof are sent back to the Verifier.

⑤ The verifier applies ZK Proof Verification algorithm to ensure the response is correct. If the algorithm gives positive answer, the verifier trusts the response as if it has been produced by Trusted Third Party

Benefits of Zero Knowledge Proofs (ZKPs)

① Simple

- One of the prime advantages of zero knowledge proof is that it does not involve any complex encryption method.

② Secure

- It does not require anyone to reveal any sort of information.

③ Lengthy

- In the zero-knowledge method, there around 2k computations, with each requiring a certain amount of time of process. This is the foremost con of going with zero knowledge proof.

④ Imperfect

- The messages delivered to verifier / prover might be destroyed or modified.

⑤ Limited

- The zero knowledge protocol demands the secret to be a numeric value. In other cases, a translation is required.

Properties of Zero Knowledge Proof

① Completeness

- If the statement is true and both users follow the rules religiously, then the verifier would be convinced without any external help.

② Soundness

- If the statement is false, the verifier won't be convinced in any scenario. (Even if the prover says that the statement is true for some small probability).

③ Zero Knowledge

- In both cases, verifier won't be able to know any information beyond that the statement is true or false.

AMEY TE B 50 Amey

Types of Zero Knowledge Proofs

① Interactive Zero Knowledge Proof

- In this, a prover performs a series of actions under the mechanism of mathematical probability to convince the verifier of a particular fact.

② Non-Interactive Zero Knowledge Proof (NIZKP)

- As depicted from the name, NIZKP does not require an interactive process.
- It means prover can generate all the challenges at once and verifier's can later respond. This restricts the possibility of collision. However, it requires additional machines and software to find out the sequence of experiments

Implementation of Zero Knowledge Proof in Blockchain System

- Messaging
- Authentication
- Storage Protection
- Sending Private blockchain transactions
- Complex documentation
- File System Control
- Security for sensitive information.

Zero Knowledge proof has the potential to enhance data privacy and security in a vast number of use cases, be it in the case of fraud prevention system requiring users' personal details or in the case of an IOT system relying upon an anonymous data.