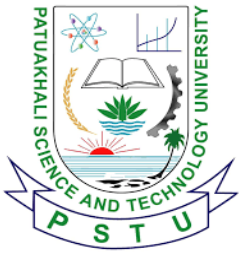
PATUAKHALI SCIENCE AND TECHNOLOGY UNIVERSITY



Assignment

Assignment on creating Questions and Answers from Research Papers
Course Title : Cryptography and Network Security
Course Code : CCE-421

Submitted to:

Golam Md. Muradul Bashir

Professor

Department of Computer and Communication Engineering

Faculty of Computer Science and Engineering (CSE)

Submitted by:

ID: 2002017, 2002033, 2002041, 2002046, 2002070

Session: 2020-2021

Level – 4 , Semester - 2

Faculty of Computer Science and Engineering (CSE)

Paper-1
Network Security and Cryptography: A Qualitative Exploration and Recent Advancements

1. Identify and explain the four fundamental security services that any cryptosystem must fulfill to ensure secure communication. **4**

Answer:

Confidentiality: This is the primary service focused on preventing unauthorized individuals from accessing information. It ensures secrecy using mathematical algorithms, fuzzy logic, and physical security.

Data Integrity: This ensures that the message is received exactly as it was sent, without any ambiguity or modification. It is maintained through checksums and error detection/correction techniques built into the algorithm.

Authentication: This service verifies the identity of the sender to discourage false or rogue communications. Digital signatures are a common modern implementation of this service.

Non-Repudiation: This prevents either the sender or the receiver from denying a previous commitment or the ownership of a message. It is essential for communications where the chance of dispute is high.

2. What are active and passive attacks? Provide an example for each. **3**

Answer:

Passive Attack: This is like "eavesdropping." The attacker quietly watches or listens to the data being sent but does not change it. Because nothing is altered, it is very hard to detect, and the message reaches its destination exactly as it was sent. The goal is to steal secrets or monitor patterns.

Example: Someone reading your private emails while they are being sent to a friend.

Active Attack: This is like "tampering." The attacker changes the data, deletes it, or sends fake messages. These attacks are easier to notice because they disrupt the service or change the information, but they are much more dangerous to the system's operation.

Example: An attacker changing the amount of money in a bank transfer message before it reaches the bank.

Paper-2
Content Security Distribution Scheme Based on Certificateless Public Key Cryptography

3. How does the certificateless mutual authentication process work? **3**

Answer:

The process begins with system initialization by the Key Generation Center (KGC), which selects system parameters and generates the master key. Users register their identity information with the KGC, which then generates public-private key pairs based on the SM9 algorithm and securely distributes private keys.

When communication begins, the client sends an authentication request to the server, including its identity and a signature created using its private key. The server verifies the signature using SM9. The server then sends back its own identity information and signature. The client verifies the server’s signature.

If both verifications are successful, mutual authentication is completed, ensuring that both parties are legitimate and preventing forgery or man-in-the-middle attacks.

4. What are the specific cryptographic functions performed by the SM3, SM4, and SM9 algorithms within the secure content distribution scheme? 4

Answer:

The proposed solution uses three domestic commercial cryptographic algorithms, each with a specific role:

- **SM4** is a symmetric encryption algorithm used to encrypt content files, ensuring that the transmitted data remains confidential.
- **SM3** is a hash algorithm used to generate a file digest (summary) of the content file, which helps verify data integrity and detect any tampering.
- **SM9** is an identity-based cryptographic algorithm used for mutual authentication, digital signatures, and secure encryption of the symmetric key. It ensures authentication and non-repudiation in the system.

Together, these algorithms provide confidentiality, integrity, authentication, and non-repudiation.

Paper-3

Quantum Cryptography: A Pathway to Secure Communication

5. What is the main purpose of Quantum Cryptography? 2

Answer:

The main purpose of Quantum Cryptography is to provide secure communication by using principles of quantum mechanics. It can detect eavesdropping because measuring quantum data disturbs it, which alerts the users.

6. Why is Quantum Computing a threat to Classical Cryptography? **2**

Answer:

Quantum Computing is a threat because a quantum computer running Shor's algorithm can break traditional encryption algorithms (like RSA) much faster than classical computers. This makes many current cryptographic systems insecure.

Paper-4

Image Cryptography using AES-256 Algorithm

7. What is AES and why is it used? **3**

Answer:

AES (Advanced Encryption Standard) is a symmetric encryption algorithm. It uses one secret key for both encryption and decryption, which means the same key is used to lock and unlock the data.

AES is widely used because it is fast, reliable, and provides strong security. AES-256, which uses a 256-bit key, offers a higher level of protection. It makes

images or other data very difficult to hack, read, or change without the correct secret key. That is why it is commonly used to protect sensitive information.

8. What are the main steps in the AES encryption process? **3**

Answer:

The main steps in AES encryption are:

- AddRoundKey – The secret key is added to the data.
- SubBytes – Each byte is replaced using a special table (S-box).
- ShiftRows – The rows of data are shifted.
- MixColumns – The columns are mixed to increase security.

These steps are repeated several times to produce the final encrypted image.

Paper-5

Implementation and Analysis of ECC (Elliptic Curve Cryptography) Security Routing Protocol in NS2

9.What is Elliptic Curve Cryptography (ECC) and why is it used in network security? **3**

Answer:

Elliptic Curve Cryptography (ECC) is a modern public-key cryptographic technique used to secure data communication in networks. It is based on the

mathematical properties of elliptic curves and provides strong security with smaller key sizes compared to traditional algorithms. ECC supports important security functions such as encryption, digital signatures, and key exchange. Because of its smaller key size, ECC requires less computational power and memory, making it suitable for wireless and resource-constrained devices. The concept of ECC was independently proposed by Neal Koblitz and Victor S. Miller. Therefore, ECC is widely used in modern secure communication systems.

10. Why is ECC preferred over traditional cryptographic algorithms like RSA in wireless networks? **3**

Answer:

ECC is preferred over traditional cryptographic methods because it provides the same level of security using much smaller key sizes. Smaller keys reduce computational complexity and improve processing speed in network devices. This is especially important in wireless networks where bandwidth, power, and memory are limited. ECC also reduces communication overhead during encryption and key exchange operations. Additionally, ECC offers strong resistance against common security attacks such as eavesdropping and impersonation. For these reasons, ECC is considered more efficient and secure than RSA in many modern network applications.