SEM 3 – NSC ( Network Security and Cryptography) Exam Questions

Question 1 . About asymmetric symmetric encryption

* Concept: Asymmetric and symmetric encryption are two primary techniques used to secure data. Symmetric encryption uses the same key for both encryption and decryption, while asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption.

Asymmetric encryption uses a mathematically related pair of keys for encryption and decryption: a public key and a private key. If the public key is used for encryption, then the related private key is used for decryption. If the private key is used for encryption, then the related public key is used for decryption.

On the other hand, the entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process

* Encoding and decoding diagram:

A diagram of keys and a key system

Description automatically generated

A diagram of keys and a keyword

Description automatically generated

* Compare:

| **Symmetric Key Encryption** | **Asymmetric Key Encryption** |
| --- | --- |
| It only requires a single key for both encryption and decryption. | It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt. |
| The size of cipher text is the same or smaller than the original plain text. | The size of cipher text is the same or larger than the original plain text. |
| The encryption process is very fast. | The encryption process is slow. |
| It is used when a large amount of data is required to transfer. | It is used to transfer small amounts of data. |
| It only provides confidentiality. | It provides confidentiality, authenticity, and non-repudiation. |
| The length of key used is 128 or 256 bits | The  length of key used is 2048 or higher |
| In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption. | In asymmetric key encryption, resource utilization is high. |
| It is efficient as it is used for handling large amount of data. | It is comparatively less efficient as it can handle a small amount of data. |
| Security is less as only one key is used for both encryption and decryption purpose. | It is more secure as two keys are used here- one for encryption and the other for decryption. |

Question 2 . Security Vulnerability

* Concept: A Security Vulnerability is a weakness, flaw, or error found within a security system that has the potential to be leveraged by a threat agent in order to compromise a secure network.
* SQL Injection and how to prevent it:

+ SQL Injection: is a code-based vulnerability that allows an attacker to read and access sensitive data from the database. Attackers can bypass security measures of applications and use SQL queries to modify, add, update, or delete records in a database. A successful SQL injection attack can badly affect websites or web applications using relational databases such as MySQL, Oracle, or SQL Server.

+ How to prevent it:

Primary Defenses:

Option 1: Use of Prepared Statements (with Parameterized Queries)

Option 2: Use of Properly Constructed Stored Procedures

Option 3: Allow-list Input Validation

Option 4: Escaping All User Supplied Input

Additional Defenses:

Also: Enforcing Least Privilege

Also: Performing Allow-list Input Validation as a Secondary Defense