Question one. ***A) briefly describe five basic at least basic security service provided by cryptography***

1. Confidentiality: This service ensures that the information being transmitted or stored is only accessible to authorized parties. This can be achieved through techniques such as encryption.
2. Integrity: This service ensures that the information being transmitted or stored has not been tampered with or altered in any way. This can be achieved through techniques such as digital signatures and message authentication codes.
3. Authentication: This service verifies the identity of the parties involved in a communication. This can be achieved through techniques such as digital certificates and biometric authentication.
4. Non-repudiation: This service ensures that the parties involved in a communication cannot deny having sent or received a particular message. This can be achieved through techniques such as digital signatures and timestamps.
5. Access Control: This service controls who has access to certain resources or information. This can be achieved through techniques such as role-based access control (RBAC) and access control lists (ACLs)

b) describe vulnerability of BGP.

Answers

BGP (Border Gateway Protocol) is a routing protocol used to exchange routing information between routers in different autonomous systems (AS) on the internet.

There are several vulnerabilities associated with BGP that can be exploited by attackers to disrupt internet connectivity, steal sensitive information, or redirect traffic to malicious actors.

1. Route hijacking: An attacker can falsely advertise a route to a specific IP address prefix, causing traffic intended for the legitimate destination to be directed to the attacker's network.
2. Route leakage: An attacker can propagate a false routing table to a neighbouring router, causing traffic to be directed to the attacker's network instead of its intended destination.
3. BGP prefix hijacking: An attacker can falsely advertise a prefix, causing traffic intended for a legitimate prefix to be directed to the attacker's network.
4. BGP route reflection amplification: An attacker can use route reflection to amplify traffic and launch a DDoS attack.
5. BGP session hijacking: An attacker can steal a BGP session by guessing or cracking the session's password, and then inject false routing information into the network.
6. BGP Configuration errors: Misconfigured BGP routers can also lead to routing loops, blackholes, and other connectivity issues.

Overall, BGP is a complex protocol and its security is largely dependent on the security of the underlying infrastructure and the proper configuration of BGP routers.

Question two: a) describe how RPKI makes BGP more secure

Answer

RPKI (Resource Public Key Infrastructure) is a set of protocols and technology that aims to improve the security of BGP (Border Gateway Protocol) by providing a secure way for Internet Service Providers (ISPs) to authenticate the origin of IP address prefixes.

RPKI uses digital certificates and public key infrastructure (PKI) to create a hierarchical trust model for BGP routing. Each ISP is issued a digital certificate by a trusted certificate authority (CA) and each prefix is assigned a digital signature by the ISP that owns it.

The main features of RPKI that makes BGP more secure include:

1. Origin Validation: RPKI allows ISPs to validate the origin of an IP address prefix by checking the digital signature on the prefix against the digital certificate of the ISP that owns it. This helps to prevent route hijacking and route leakage.
2. Prefix Validation: RPKI allows ISPs to validate that a prefix is properly authorized for use by checking the digital certificate of the ISP against a list of valid prefixes. This helps to prevent BGP prefix hijacking.
3. Route Flap Damping: RPKI allows ISPs to dampen routes that are frequently changing, reducing the impact of BGP route reflection amplification attacks.
4. Router Authentication: RPKI allows ISPs to authenticate BGP routers, preventing unauthorized routers from injecting false routing information into the network.

In summary, RPKI is a key technology that can help improve the security of BGP by providing a secure, globally-coordinated way to authenticate the origin of IP address prefixes and routers, thus reducing the risk of routing-based attacks and improving the overall stability of the internet routing.

B) mention at least 4 protective measure that may be taken in order to minimize the likelihood of a key compromise.

Answers

There are several protective measures that can be taken to minimize the likelihood of a key compromise in a cryptographic system:

1. Key management: Properly managing the generation, distribution, storage, and destruction of keys is crucial in preventing key compromise. This includes using strong key generation algorithms, implementing secure key distribution methods, and storing keys in secure locations.
2. Access control: Implementing strict access controls for key management systems and key storage locations can help to prevent unauthorized access to keys. This includes providing access only to authorized personnel and implementing multi-factor authentication methods.

3. Key backup and recovery: Having a secure key backup and recovery plan in place can help to minimize the impact of a key compromise by quickly replacing compromised keys.
4. Regular key rotation: Regularly rotating keys can reduce the risk of key compromise by limiting the amount of time a key is in use and reducing the potential impact of a compromise. This can be achieved by using short-lived keys or scheduling regular key replacement.
5. Physical security: Keeping the systems and devices that hold the keys physically secure is important, as it limits the risk of unauthorized access to the keys. This includes using tamper-evident seals, monitoring the devices with surveillance cameras and ensuring that only authorized personnel have access to the location where the devices are stored.
6. Cryptographic agility: Having the ability to switch to new cryptographic algorithms and protocols quickly in case of a vulnerability or key compromise.

Overall, it's important to have a comprehensive key management plan in place that addresses all aspects of key security, including generation, distribution, storage, and destruction of keys.

Question three: A) mention at least 4 popular example of NoSQL database

Answers

NoSQL databases are non-relational databases that are designed to handle large amounts of unstructured or semi-structured data. There are several different types of NoSQL databases, each with its own strengths and weaknesses. Here are four popular examples of NoSQL databases:

1. MongoDB: MongoDB is a document-based NoSQL database that is known for its scalability and flexibility. It uses a JSON-like data model and supports dynamic schema, making it well-suited for applications that require real-time data processing and analytics.
2. Cassandra: Cassandra is a wide-column store NoSQL database that is known for its high performance and scalability. It is designed to handle large amounts of data across multiple commodity servers, making it well-suited for use cases such as real-time analytics and internet-of-things (IoT) data.
3. Redis: Redis is an in-memory key-value store that is known for its high performance and low latency. It is often used for caching, real-time analytics, and other use cases that require fast data access.
4. Riak: Riak is a distributed key-value store that is known for its high availability and fault tolerance. It is designed to handle large amounts of data across multiple servers, making it well-suited for use cases such as distributed systems and cloud computing.

These are just a few examples of the many different types of NoSQL databases that are available. Depending on your use case, other types of NoSQL databases such as graph databases, document-oriented databases or time-series databases may also be suitable.

B) with vivid example, describe at least six method to secure databases.

Answers

Securing databases is critical to protecting sensitive information and maintaining the integrity and availability of data. Here are six methods that can be used to secure databases, along with examples of how they can be applied:

1. Encryption: Encrypting sensitive data in the database can protect it from unauthorized access, even if the database is compromised. For example, a healthcare provider could encrypt patient medical records in its database to protect them from unauthorized access.
2. Access Control: Implementing strict access controls can prevent unauthorized users from accessing the database. For example, a company's HR database could be configured to only allow HR employees to access employee information, while denying access to other employees.
3. Firewalls: Firewalls can be used to restrict access to the database server by only allowing authorized traffic through. For example, a financial institution could use a firewall to only allow traffic from their internal network to access their financial databases.
4. Data masking and tokenization: This method involves replacing sensitive data in the database with non-sensitive data, such as tokens or random values, making it unreadable to unauthorized users. For example, a credit card company could use data masking to protect sensitive credit card information by replacing the actual numbers with tokens.
5. Regular backup and disaster recovery: Regularly backing up the database and having a disaster recovery plan in place can minimize the impact of a data breach or other security incident. For example, a retail company could have a disaster recovery plan in place that includes regular backups of their inventory database and a plan for restoring the data in case of a security incident.
6. Auditing and monitoring: Keeping track of database activity by auditing and monitoring can help identify and respond to security incidents. For example, a government agency could use auditing and monitoring to keep track of access to sensitive information in its databases, such as immigration records.

It's important to note that no single method can provide complete protection for a database, so a combination of methods should be used to secure the database and protect the data.