LEMUEL OKECHUKWU

VEPH/20B/CY082

TASK 24B

DATA MASKING

**TASK 24B:**

* **Define Data masking?**
* **Using kali linux , embed the following text.(my laptop pin  is 4457),**

**( my ssn is 987533261) (my bvn is 12475883) in 3 different images and write technical reports on how it was carried with pictorial evidence and how it was carried out. kindly reconstruct this message and make it technical**

[](https://www.zendata.dev/post/data-masking-what-it-is-and-8-ways-to-implement-it)

As technology advanced and data became more valuable and vulnerable, traditional security measures such as encryption and access controls proved insufficient for protecting data at rest or in transit. Further, they have also exploded in volume, introducing new[vulnerabilities.](https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-a-security-vulnerability/)

Therefore, data masking emerged as a proactive approach to data security, offering a way to protect sensitive information without compromising its utility. Initially used primarily in software testing and development to anonymize sensitive data for testing purposes, data masking gradually expanded its use cases to include areas such as data warehousing, analytics, and compliance.

**Data masking** is a security technique used to protect sensitive information by replacing or obscuring it with fictitious or anonymized data. It ensures that sensitive data remains confidential while allowing organizations to use it for legitimate purposes such as testing, development, analytics, or sharing.

Types of Data Masking: there are several types of data masking techniques which are unique in their little ways and their scope.

1. **Shuffling:** involves randomly reordering the values of sensitive data within a dataset while preserving the overall statistical properties. This means that individual records become difficult to identify, but the integrity of the dataset remains intact.
2. **Substitution:** In this technique, sensitive data is replaced with fictitious but realistic-looking data. For example, instead of using real names, you might replace them with randomly generated names. Similarly, you could replace credit card numbers with fake but valid-looking numbers.
3. **Masking:** ensures that sensitive information remains concealed from unauthorized users while allowing authorized users to access the necessary data, protecting your data privacy and security.  For instance, you could mask credit card numbers except for the last four digits.
4. **Tokenization**: is commonly used in payment processing and other applications where sensitive data needs to be securely handled. It protects data from unauthorized access and ensures compliance with data protection regulations.

Others are Hashing, Perturbation and Encryption.

Some of the most notable applications of data masking include:

Testing and Development - Data masking ensures that sensitive information like personally identifiable information (PII), financial data, or healthcare records are altered or replaced with fictitious yet realistic data. This process typically involves using masking algorithms to preserve data format and relationships while obscuring sensitive values.

Analytics and business intelligence - Techniques such as tokenization or encryption may be employed to anonymize data, allowing for analysis while preserving confidentiality.

Data warehousing and data lakes - Organizations apply masking techniques to anonymize sensitive data before loading it into repositories like[warehouses and lakes](https://www.spiceworks.com/tech/big-data/articles/data-lake-vs-data-warehouse/). This involves altering or obfuscating values using methods like substitution or tokenization, preserving data integrity while adhering to data privacy regulations.

As data landscapes evolve, data masking is transforming to meet emerging challenges. Future trends suggest a move towards AI-powered masking, where machine learning algorithms dynamically optimize data protection strategies. This promises more accurate, efficient, and adaptive solutions to safeguard sensitive information against evolving threats.

* [Data Privacy and the Journey of Smarter Security](https://www.spiceworks.com/it-security/data-security/articles/the-data-privacy-journey/)
* [What is Data Anonymization? Importance, Tools, and Use Cases](https://www.spiceworks.com/it-security/data-security/guest-article/what-is-data-anonymization/)