The practice of using algorithms to encrypt and decrypt data, ensuring secure communication and data protection. It transforms readable data (plaintext) into an unreadable format (ciphertext), which can only be deciphered by the intended recipient with the correct key. This process safeguards data from unauthorized access and tampering, maintaining its confidentiality, integrity, and authenticity.

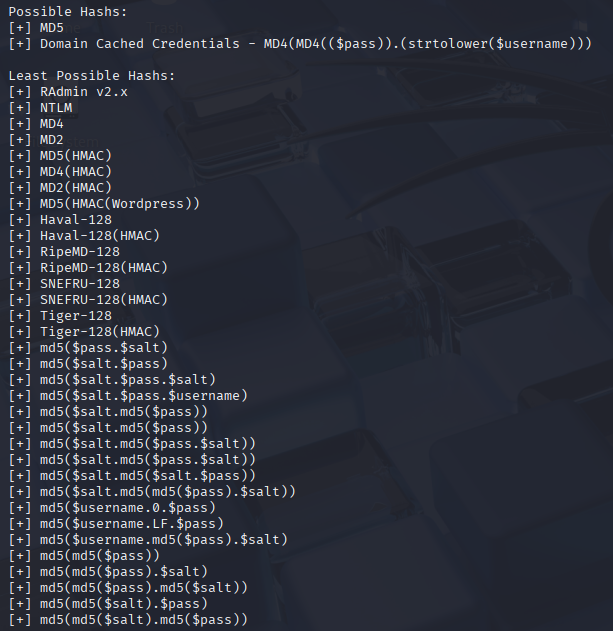
**HASHING :** Hashing is a cryptographic technique used to convert data of any size into a fixed-size string of characters (a hash or hash value) using a hash function. It's a one-way process, meaning the original data cannot be easily recovered from the hash. Hashing is crucial for ensuring data integrity and security, especially in password storage and digital signatures. Md5, sha-1, sha-256, sha-512 are the hashing algorithms used.



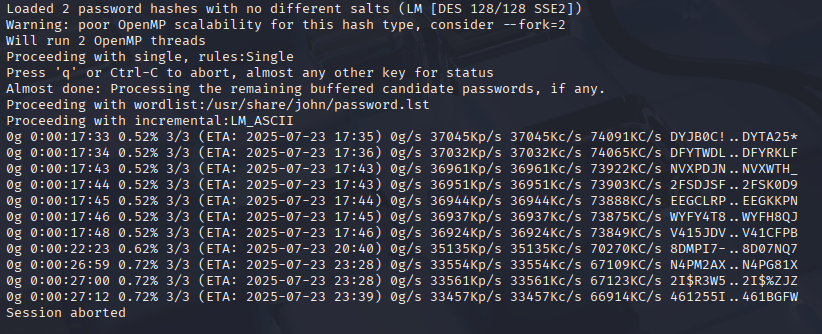
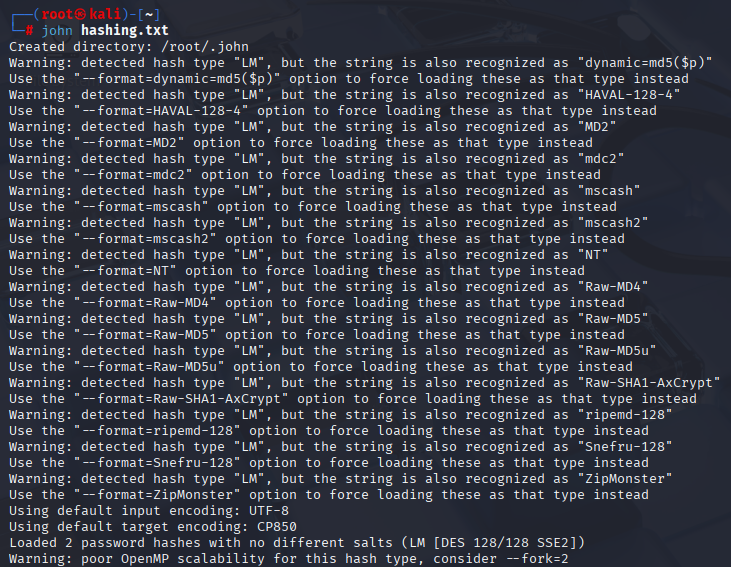
By using the algorithm the text got converted into hash value. as we can also see the length of the string increases as we change the algorithm.

Hash-identifier is a tool used to identify which type of algorithm they used for encryption as shown in snapshot, it identified as “md5” algorithm.





Here we are using john the ripper to decrypt the data by brute forcing. As shown in the snapshot below.



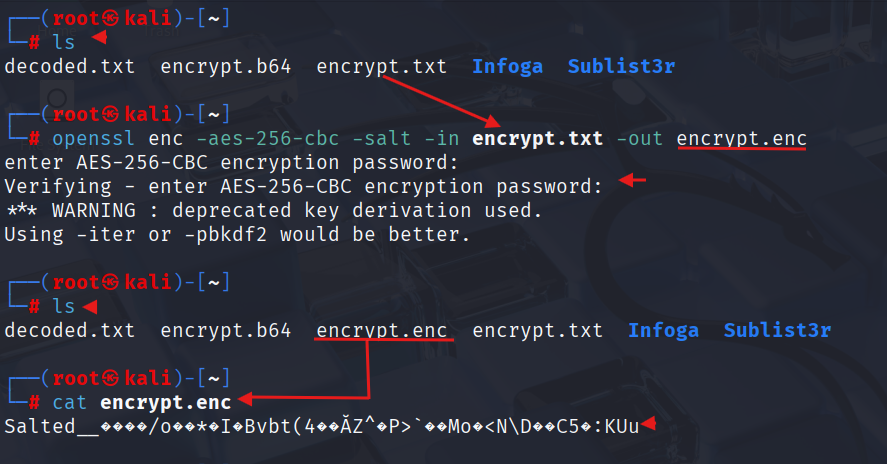
**ENCRYPTION :** The process of converting information into a secret code, making it unreadable to unauthorized individuals. This process ensures that even if data is intercepted or accessed by malicious actors, it remains unintelligible and unusable without the decryption key.

* ***Symmetric* :** A type of encryption that uses a single, shared key for both encrypting and decrypting data.

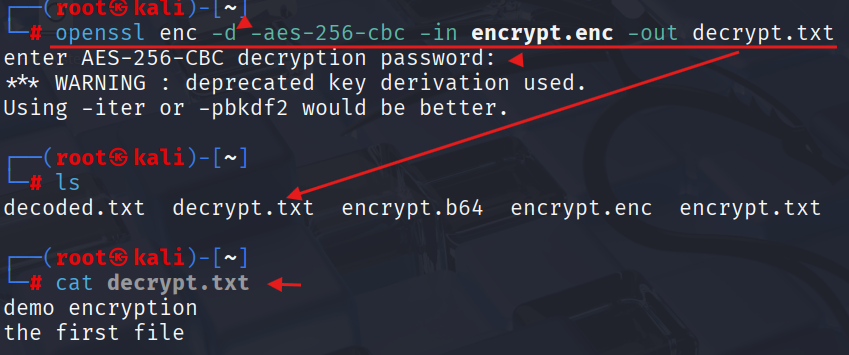
For encryption we have openssl along with algorithm “aes” bit “256” type of encryption is cbc cipher,then we add salt to randomize the text file then will add the file name Example : openssl enc -aes-256-cbc -salt -in filename.txt -out filename.enc

This command will encrypt the data to decrypt it we need to know which algorithm have been used and we need the key to decrypt it.

**Encryption :** As shown in the snapshot.



**Decryption :** As shown in the snapshot.

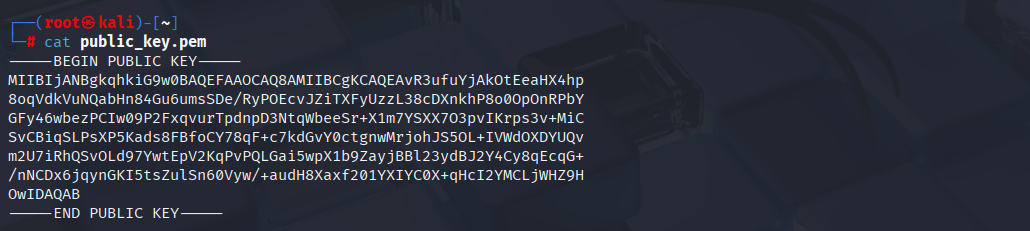


* ***Asymmetric* :** A type of encryption that uses a pair of keys – a public key and a private key – for encrypting and decrypting data. The public key can be shared openly, while the private key must be kept secret by its owner.

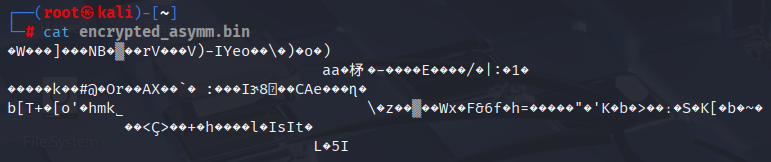
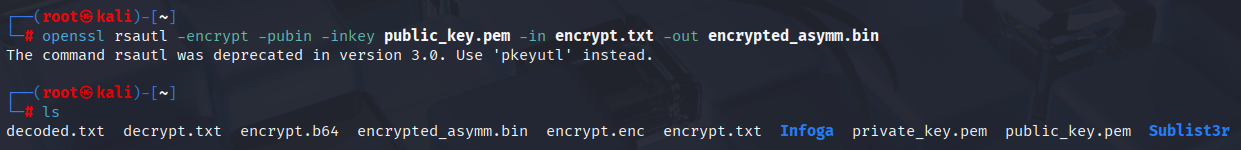
we have openssl along with algorithm “RSA” to create a private key and to store the data in a private\_key.pem file we use the following command as shown Example : Openssl genpkey -algorithm RSA -out private\_key.pem, Then this command generates the private\_key as shown in the snapshot.



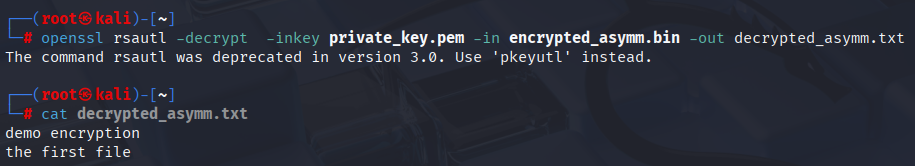
Now we need to pull out the public key from the file private\_key.pem as shown in the above snapshot at the bottom after creating the private key. In the below snapshot we can see the public key that we pulled from private and stored it in public\_key.pem by using cat command.



Now we will encrypt the file by placing the public key in it and store the output in a file as shown in the snapshot. By using cat command we can see the encrypted data of a file we created.



To decrypt the file we using private key filename (private\_key.pem) on the encrypted filename (encrypted\_asymm.bin) to get the output in the filename (decrypted\_asymm.txt) as shown in snapshot.

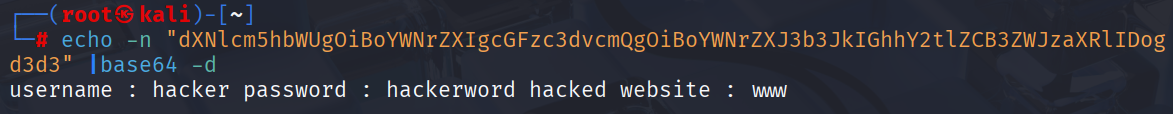
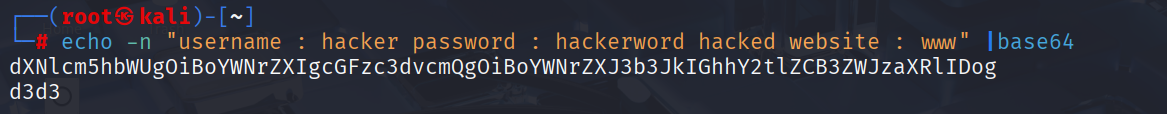


In summary it takes the data from encrypted\_asymm.bin, uses the private\_key.pem to decrypt it using the RSA algorithm, and then writes the original, unencrypted data to decrypted\_asymm.txt.

**ENCODING :** The process of converting data into a specific format for different purposes, such as storage, transmission, or processing. It involves using algorithms or rules to transform data into a format that is more suitable for a particular system or medium. encoding is not primarily a security mechanism.

**EXAMPLES :** In first case we did encoding for the text, In the second case we did encoding for a file.

**FIRST CASE :**



**SECOND CASE :**

