Private key

- Private keys are used to authorize transactions and prove that your coins, tokens, NFTs that are in your wallet are owned by you.
- Metamask seedphrase (the 12 word job, the one that no one should lose nor share with anyone) generates a set of private/public key pairs, each address (account) in MM gets a single pair of private keys, basically whenever you approve a swap, transaction or any other interaction through mm you sign it with your private key.
- A bit more advanced - private key is an alphanumeric string with a length of 32 bytes, no more, no less. Unless you get in to the EVM world of writing smart contracts this is not too relevant.
- If one really wants to see his private key it can be done in MM, but there is no need to keep that secure (see second bullet point)