The three parts of a JSON Web Token, or JWT, are header, payload, and signature. A header usually describes the type of token and the algorithm being used. It is Base64Url Encoded. Payloads are also Base64Url Encoded and contain claims. Claims are information about an entity. Signature incorporates the header and payload to verify the message and sender. The algorithm noted in the header is used to generate the signature.

https://jwt.io/introduction

https://www.ibm.com/docs/en/cics-ts/6.1?topic=cics-json-web-token-jwt

https://fusionauth.io/articles/tokens/jwt-components-explained

Hashing and salting are both methods of making plaintext, like passwords, secure. Salting is when random characters are added to a password string, either at the beginning or end. Hashing is when the plaintext is converted by an algorithm into unrecognizable text, which cannot be reversed. To add extra security, salting and hashing are sometimes used together.

https://www.tokenex.com/blog/ab-hashing-vs-salting-how-do-these-functions-work/#:~:text=Hashing%20takes%20plaintext%20data%20elements,in%20order%20to%20decode%20it.

https://www.pingidentity.com/en/resources/blog/post/encryption-vs-hashing-vs-salting.html

https://cyberhoot.com/cybrary/password-salting/