**Explore different types of cryptographic methods.**

[- Single key encryption

- Private+Public Key encryption

-Hashing

-Digital Signatures]

The field of cryptography encompasses various methods and techniques for securing data and communications through encryption and decryption. the most popular types of cryptographic methods are:

1. Symmetric Encryption: Symmetric encryption, also known as secret-key encryption, involves the use of a single secret key for both encryption and decryption of data. The same key is shared between the sender and the recipient. Eg. Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES).

2. Asymmetric Encryption: Asymmetric encryption uses a pair of keys: a public key and a private key. The public key is widely distributed and used for encryption, while the private key is kept secret and used for decryption. Data encrypted with the public key can only be decrypted with the corresponding private key, and vice versa. Eg. RSA (Rivest-Shamir-Adleman) and Elliptic Curve Cryptography (ECC).

3. Hash Functions: Hash functions are one-way cryptographic algorithms that generate a fixed-size hash value or digest from input data of any size. Hash functions are commonly used for data integrity verification and password hashing. Eg. SHA-256, MD5 etc.

4. Digital Signatures: Digital signatures provide a mechanism for verifying the authenticity, integrity, and non-repudiation of digital messages or documents. Digital signatures use asymmetric encryption to generate a unique cryptographic signature for a given message or data set. The sender's private key is used to sign the message, while the recipient can verify the signature using the sender's public key. Digital signature algorithms include RSA, DSA (Digital Signature Algorithm), and ECDSA (Elliptic Curve Digital Signature Algorithm).

**Check demo of hashing:**

**https://tools.superdatascience.com/blockchain/public-priva te-keys/keys**

[- Checked]