**Encryption/Decryption**

**Encryption**

**Encryption** is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting **plaintext** (the original bytes (text, image, etc.)) to **ciphertext** (encrypted text). In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of an **encryption key** that is a set of mathematical values known only by the sender and the recipient of the encrypted message know.

|  |
| --- |
| *Encryption example* |

**Q: What is plaintext or cleartext?**A: The decrypted message, when it is returned back into its plain or original state of context which is comprehensible and decipherable, is also known as cleartext or plaintext.

 - Interview Q&A

**Q: What is ciphertext?**  
A: When the message is encrypted into a state which is totally incomprehensible and indecipherable, this is known as the ciphertext. So, to illustrate all of this, with the previous example, when the sending party creates the written message of “I LOVE YOU”, this is the plaintext or the cleartext. Once this message is encrypted into the format of “UYO I VEOL” and while it is in transit, it becomes known as the ciphertext. Then, once the receiving party gets this ciphertext and then decrypts it into a comprehensible and understandable form of “I LOVE YOU,” this message then becomes the plaintext or the cleartext again.

**Decryption**

**Decryption** is a process of converting encoded/encrypted data (ciphertext) in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using keys that were used to encrypt the original data.

| **https://docs.google.com/uc?id=1TWp9M2gU1jPPvrhgPWC10hbSc9OMsfYK** |
| --- |
| *Decryption example* |

**Q: What exactly are encryption and decryption?**  
A: The terms “scrambling” and “descrambling” are commonly known as “encryption” and “decryption.”  
For example: when the written message “I LOVE YOU” is scrambled by the sending party, it becomes what is known as the “encrypted message.” This means that the written message has been disguised in such a manner that it would be totally meaningless, or in the terms of cryptography, it would be undecipherable.  
Encryption can also be described as the conversion of information from a readable state to apparent nonsense. When the receiving party receives this encrypted written message, it must be unscrambled into an understandable and comprehensible state of the context. This process of unscrambling is also known as decryption

**Hashing**

Hashing is the process of converting a given key to another value. A **hash function** is used to generate the new value according to a mathematical algorithm. The result of a hash function is known as a **hash value** or simply, a **hash**.

Hashing is also used in data encryption (we will learn in the following lessons). Passwords can be stored in the form of their hashes so that even if a database is breached, plaintext passwords are not accessible. **MD5**, **SHA-1** and **SHA-2** are popular cryptographic hashes.

| **https://docs.google.com/uc?id=1SBmIKZN8PzETVCKBWcq4HSpSxhDqI2C7** |
| --- |
| *Hashing Example* |

**Q: What is the hashing function?**A: The hashing function is a one-way mathematical function. This means that it can be used to encode data, but it cannot decode data. Its primary purpose is not to encrypt the ciphertext; rather, its primary purpose is to prove that the message in the ciphertext has not changed in any way, shape or form. This is also referred to as “message integrity.” If the mathematical function has changed in any way, the message has then changed.

**Cryptocurrency**

**Cryptocurrency** is an internet-based medium of exchange which uses cryptographical functions to conduct financial transactions. Cryptocurrencies leverage blockchain technology to gain decentralization, transparency, and immutability.

**Blockchain** is the technology that enables the existence of cryptocurrency. **Bitcoin** is the name of the best-known cryptocurrency, the one for which blockchain technology was invented. A cryptocurrency is a medium of exchange, such as the US dollar, but it is digital and uses encryption techniques to control the creation of monetary units and to verify the transfer of funds.

| **https://docs.google.com/uc?id=1t-_RT7tIxMZYDrYPFaxwzDM3hitLDmGA** |
| --- |
| *Cryptocurrency* |