Basics of Encryption and Decryption

Meaning of Encryption

Encryption is a method of mixing data so that only authorized parties can understand the information. Technically, it is the process of converting plain text into cipher text. In simpler terms, encryption takes readable data and changes it so that it appears randomly. Encryption requires the use of an encryption key: a set of mathematical values that both the sender and recipient know of the encrypted message.

Although the encrypted data appears to be random, the encryption continues in a logical and predictable manner, so the party receiving the encrypted data and in possession of the key used to encrypt the data can decrypt the data and convert it back into plain text. Really secure encryption will be complex enough that it is unlikely that a third party will decrypt the encrypted text with brute force - in other words, by guessing.

Data can be encrypted "at rest", when stored, or "while in transit", while it is being sent elsewhere.

Benefits of Encryption

Data breaches are becoming more and more common in today's society. Hackers know that they can sell hacked information on the dark web or use it for purposes like blackmail.

However, encryption technology for data protection is widely available. It involves protecting information with encryption via encrypted code. Only people who have the key to decrypt the data can read it. Here are seven reasons to rely on encryption technology:

1. You Can Use It across a Variety of Devices

One of the most important advantages of modern encryption technology is that you can apply it to all or most of the technical devices you use. Data on iPhone is encrypted by default as long as you lock it with a password or Touch ID. On an Android phone, it's easy to walk through an encryption process under the Security menu of the Settings section. Encryption is enabled on some Android devices upon purchase.

There are free and paid options for encrypting your computer as well. Depending on your needs, companies offer full encryption on your hard disk or file. Also, do not ignore the options available to encrypt the content on the SD card or thumb drive. Since there are so many possibilities for people who want to encrypt their data, at least it is worth researching to find ways that are best for you. Internet traffic must also be encrypted. Most secure VPN providers always use the 256-bit encryption protocol.

2. It Helps You Stay Safer When Working Remotely

Companies now repeatedly require workers to only use encoded devices due to accidents like this. This is not surprising, considering how other technological developments make it easier for employees to keep productivity from anywhere.

However, according to the 2018 North American Report published by Shred-It, most business leaders believe that the risk of data breach is higher when people work remotely. More specifically, 86% of C-Suite executives and 60% of small business owners have this opinion. Whether you work remotely all the time or from time to time, data encryption helps you prevent information from falling into the wrong hands.

3. It Supports Data Integrity

Another thing to remember about encryption technology to protect data is that it helps to increase the integrity of the information alone. In fact, encryption alone does not guarantee this, but it is something you can and should use as part of a comprehensive strategy. If you trust the data, it is easy to use it with confidence to make business decisions.

Statistics indicate that poor data quality is the primary reason why 40% of all business initiatives fail to achieve their targeted benefits. High-quality information can help you learn more about your customers, track trends, and know things you might miss. Often companies deploy technologies such as data cleaning to improve quality, which is a good start.

Data encryption can help ensure that only authorized parties have access to company information for analysis. It also reduces the possibility of a hacker successfully manipulating data, and those actions are not observed.

4. Data Encryption Is a Privacy Safeguard

Consider the information that you have stored on your smart phone or computer, and you may understand why encryption keeps your identity secure with your data. On a smart phone, for example, encryption apps can make it virtually impossible, or at least an exceptional challenge, for anyone who is not authorized to access your information. In many cases, law enforcement officials have had difficulty investigating phone data on encrypted devices.

For ordinary users who are not usually worried that their phones become evidence, data encryption can prevent sensitive details from appearing online without knowing. Once hackers compromise information such as email addresses, legitimate owners may not know what happened until months have passed.

5. Data Encryption Could Provide a Competitive Advantage

Because data encryption applies to both information in the event of rest and transit, it provides consistent protection that can lead to peace of mind for the people who handle the information.

Research shows that growing percentage of companies know that creating an encryption plan is necessary. A 2019 study presented by the Ponemon Institute found that during FY18, 45% of surveyed companies reported that they have a comprehensive coding strategy that is constantly being applied across their organizations. Just below (42%) reported a limited encryption strategy used for specific applications or types of data.

Meaning of Decryption

Decoding is the process of taking cipher text, cipher, or other data and converting it back into text that you or your computer can read and understand. This term can be used to describe a method for manually decrypting data or decrypting data with appropriate symbols or keys.

Data may be encrypted to make it difficult for someone to steal the information. Some companies also encrypt data for the general protection of company data and trade secrets. If this data needs to be viewable, it may require decryption. If a pass code or decryption key is not available, special software may be required to decode data using algorithms to break through the decryption and make the data readable.

Advantages and Disadvantages of Decryption

The reason for using decoding varies; however, adequate security is an unambiguous advantage of decoding. This method gives the organization precisely smooth management. It is easy to see that the system can benefit security professionals because it avoids using encryption to interfere with the duplication of accurate information.

Decoding defects are basically double. The first concerns privacy, if a company chooses to use decryption; it runs the risk of separating an essential part of the workforce. In the event that the employee, by checking his email or bank details, he may discover that it is difficult to ever cause a firewall because of any insufficiently defined keywords. Consequently, the privacy expectation of the end consumer is discarded when decoding is implemented, due to inexperienced onlookers who have no concern about exposing accurate organizational data their network traffic may be monitored as a result of involuntary firewall activation.