Role of Cryptography in Protecting Data

By Dheraya Samir Kamdar
Shah and Anchor Kutchhi Engineering College (SAKEC), Mumbai
Subject:Cryptography & Network Security

Data has become one of the most vital resources in today's technological era. With the advent of the digital age, all forms of information whether for personal use, transactions, businesses, or the government have been converted into digital formats. The transition to digitalization has made life simpler and more convenient; however, the rise of cyber risks including hacking, breaches, identity thefts, and others poses a serious threat to information security. In order to protect data, it is essential to employ various methods and one such method involves using cryptography.

The term cryptography refers to a technology that involves securing information by encrypting the readable data referred to as plaintext into a format which cannot be deciphered by anyone other than those who have the appropriate decryption keys. It works on the principle that it prevents anyone from accessing the sensitive data as it is secured by encryption and thus makes it a very strong means to protect information. One of the most common real-world applications of cryptography is through messaging apps like WhatsApp wherein messages are secured and are only accessible by the parties involved.

There are many kinds of cryptography which help in protecting our information from any third party. Out of all the techniques, encryption is one of the most useful. Encryption can be classified into two broad categories that include symmetric encryption and asymmetric encryption. In symmetric encryption, there is only one key which encrypts and decrypts data. Symmetric encryption technique is very efficient, but the main issue here is the exchange of the key between the sender and receiver.

In contrast to symmetric encryption, asymmetric encryption technique involves two kinds of keys; one is a public key and another is a private key. Public key will be responsible for the encryption of the message, whereas private key will perform the decryption of the message. It should be noted that asymmetric encryption is very secure as the key is not disclosed to anyone.

Other than encryption, hashing is also an essential concept within cryptography. A hash function maps input data into a string of characters of a fixed size referred to as a hash value. One characteristic of hash functions is that any small change made to the input will lead to a completely new hash value. Hashing is therefore an excellent method for ensuring data integrity since, if there are no changes to data after being sent to a receiver, then the hash values will be identical.

Authentication and digital signatures are other applications of cryptography. Cryptography techniques can be employed to verify the identity of users as well as verify the authenticity of data/documents sent between parties. For instance, when you connect to a secure website, a

cryptographic protocol is used to authenticate that the website is indeed what it claims. Digital signatures are used to ensure data integrity within various systems such as emails and software downloads.

One of the other areas where cryptography finds wide application is securing online transactions. Anytime a person engages in an online transaction such as a payment or entering financial data, the transaction needs to be done in a secure manner. If this were not the case, it would make fraud easy to perform, causing people to suffer monetary losses. Hence, cryptography plays an indispensable role in enabling the security of online banking and e-commerce.

Even though it has many strengths, cryptography is far from being perfect. For instance, the use of weak encryption techniques, failure to implement them properly, flawed key management strategies, and human error can still pose serious risks. For example, using simple passwords or distributing keys in an unsafe way makes it possible for intruders to gain access to confidential information. As such, it is imperative to adopt high-end encryption standards, keep security systems up-to-date, and apply best practices.

Finally, cryptography faces new challenges as technology advances. In particular, the emergence of quantum computing poses a threat to encryption methods currently in use. Indeed, researchers have already begun looking at how to overcome this problem through post-quantum cryptography.

Conclusion: In summary, the application of cryptography in current cybersecurity practices has become inevitable. Apart from being a means of protecting the confidentiality of information, it also ensures the privacy, integrity, and safe transfer of data. Cryptography has found its way into everyday uses such as chat apps and e-banking, among others. As the level of cyber attacks increases, so does the significance of cryptography.