End-to-end encryption:

End-to-end encryption is an encryption standard that focuses on protecting the exchange of data from device to device. Data is encrypted on the sender’s device and is only ever decrypted on the recipient’s device. This is unlike traditional encryption practices that focus on safeguarding data in transit. End-to-end encryption is distinct from these encryption practices because not only is the data encrypted in transit, it is also never decrypted on the server.

The device-level security of end-to-end encryption is achieved using an individual’s unique public and private key pair to encrypt and decrypt data. These keys are generated whenever a new account is formed. When someone wishes to send an email or file to a colleague, that data is encrypted on the sender’s endpoint by downloading the colleague’s public key which is stored on the server. This public key can be shared with everyone. The private keys, however, are securely stored on the colleague’s device and are only available to that individual. This private key is used to decrypt the data. This encryption process establishes a secure communication channel that safeguards sensitive information.

By storing the user’s private cryptographic key on their endpoint, the keys are never available to the server. Since the server cannot access the decryption keys, it can never decrypt the data which means that criminals and nosy third parties cannot see the data either. Therefore, it offers individuals and businesses a powerful way to exchange information and store sensitive data without sacrificing privacy or security.

End-to-end encryption example

End-to-end encryption is designed so that the information exchanged between parties remains inaccessible to anyone who is not the intended recipient. Let’s go step-by-step through the end-to-end encryption process using an example:

Alice and Bob create accounts on the system. The end-to-end encrypted system provides each with a public-private key pair, whereby their public keys are stored on the server, and their private keys are stored on their device.

Alice wants to send Bob an encrypted message. She uses Bob’s public key to encrypt her message to him. Then, when Bob receives the message, he uses the private key on his device to decrypt the message from Alice. When Bob wants to reply, he simply repeats the process, encrypting his message to Alice using Alice’s public key.

In this example, end-to-end encryption operates by encrypting the data at the sender’s endpoint and decrypting it only on the intended recipient’s device. This guarantees that the data remains confidential throughout the transmission process, making it impossible for unauthorized parties to access the information being exchanged.

Securing Conversations with End-to-End Encryption

WhatsApp exemplifies how end-to-end encryption is implemented within secure messaging apps. When a user sends a message, the app encrypts the information using a unique private encryption key on the sender’s device. This encrypted message is transmitted over the internet and can only be decrypted on the receiver’s device, which possesses the corresponding private decryption key. This means that even if the message is intercepted during transmission or on the server, it remains encrypted and unreadable to anyone who needs the appropriate decryption key. WhatsApp uses end-to-end encryption to maintain the confidentiality of its users’ conversations.

Link Encryption:

Link Encryption is a technique in which a communication traveling along a network is encrypted and decrypted at every stage, or node. It is used to prevent traffic analysis and avoid human error.

With link encryption, a communication is encrypted at each node such as devices and network switches. At these points all of the information, including the header and routing information, undergoes this process.

An advantage of link encryption is the fact that the encryption occurs automatically. This reduces the risk for human error. Another is that, if the communications link operates continuously and the traffic level does not vary, then link encryption is resistant to traffic analysis.

Link encryption differs from end-to-end encryption in that, with end-to-end encryption , the internal message but not header and routing information is encrypted. end-to-end encryption also ensures that the plaintext entered into the encryption system is only visible to the sender and recipient.