October 2021

DOT Europe paper

Encryption and end-to-end encryption: a primer

Encryption measures are vital tools in protecting the privacy and fundamental rights of citizens and businesses online, allowing for secure communication and transmission of data, protecting personal and sensitive information from third party access. However, law enforcement authorities often report increased difficulty in tracking and accessing evidence of illegal activities online where encryption is involved. Discussions surrounding encryption are thus often linked to the technology's trade-off with privacy, as well as the protection of fundamental rights and the fight against illegal activities taking place online.

Given the topic's technical nature**, it is important to have a clear understanding of what encryption is, how it works, what different approaches to encryption exist and what they entail**. DOT Europe, the leading voice of digital online tech companies in Europe, would like to contribute to this important debate in order to inform legislative initiatives in this area. To that end, this document provides an overview of encryption practices, their differences and common areas of application.

How does encryption work?

Encryption is the process of scrambling data, such as text, into an unreadable form known as ciphertext, which is then decrypted by an intended recipient into its original format. This works by using an encryption key – a random string of bits generated by an algorithm – to decrypt the data and make it usable. The degree of complexity of the encryption key determines the method's security level, for example the Advanced Encryption Standard uses 128-, 192- or 256-bit keys to encrypt and decrypt data. There are two main approaches to encryption: symmetric encryption and asymmetric encryption.

Symmetric encryption

In symmetric encryption, a single key, which is exchanged between the sending and receiving parties, is used to both encrypt and decrypt the data in question. Symmetric encryption is an older method of encryption which has the benefit that the processes of encryption and decryption are very fast and efficient since the keys used in the process are comparably short. Therefore, it is typically used when large amounts of data are transferred.

However, as stated above, for symmetric encryption to function, the key must be transmitted between the involved parties. This creates a vulnerability for the security of the service as the transmission of the key could be intercepted by a third party which would allow them to decrypt shared data and access the contents.

Asymmetric encryption

In asymmetric encryption, two different keys are used respectively to encrypt and decrypt the data. This means that each recipient possesses two keys. The first key, often referred to as the public key, is shared with the sender of information. This key can then be used by the sender to encrypt the information before it is sent to the recipient. To decrypt the information, the recipient then must use their second key, often referred to as the private key. This system means that the key that is necessary to decrypt a message does not get shared with another party, thereby eliminating the risk of a third-party interception, and making the communication much more secure.

The most well-known example of asymmetric encryption is end-to-end encryption. Given the added security of this form of encryption over symmetric encryption, it is frequently used in private messaging applications and other direct communication services. However, this added security comes at the cost of decreased speed when it comes to decrypting and encrypting data.

Introducing a ‘backdoor’ or ‘master key’

It is often suggested to introduce a ‘backdoor’ or ‘master key’ that law enforcement or other public authorities could use to decrypt any piece of content within a given system. However, **implementing such a backdoor would increase the likelihood of cyber-attacks and undermine the security of encryption technology**. Terrorists and cybercriminals would target public authorities seeking to gain access to the backdoor, with possible severe outcomes for critical infrastructure and national security. Furthermore, it would **create a threat to civil liberties from governments seeking to eavesdrop on citizens**.