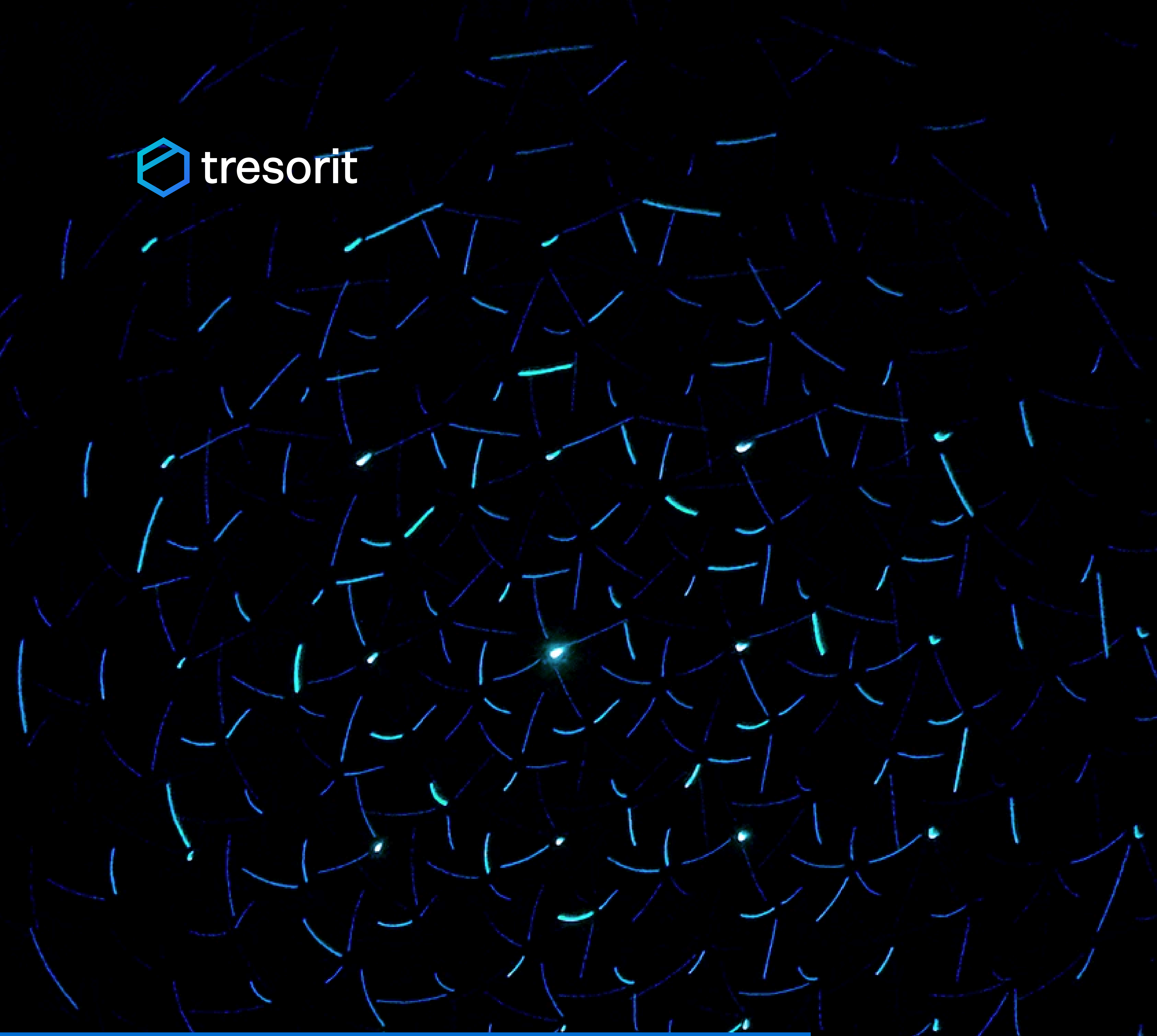


tresorit

eBook

The CIO Guide to Information Security

eBook

The CIO Guide to Information Security

Here’s what vendors don’t want you to know about encryption

Organizations are not just advised or recommended but strictly mandated to do everything in their power to ensure the security of business-critical information at all-time. It is laid out in company policies, as well as industry specific and even government-issued compliance regulations. Currently, the most advised solution for ensuring information security is encryption; the process of rendering information completely unreadable for unauthorized individuals. The problem with encryption is that there is a great deal of confusion surrounding the technology due to the many variants out on the market. Encryption is frequently used as a general term and sometimes considered the "be all and end all" solution for information security. In reality, encryption comes in all shapes and sizes and the differences must be understood when choosing the right one for the job. Putting it simply, if you are unable to differentiate between various types of encryption, your organization may end up only partially securing information by unnecessarily exposing it during its life cycle. This guide is meant to cut through all the noise and provide a clear description on how to guarantee constant information security with the holy grail of encryption; end-to-end encryption.

01

The fundamentals of information

Why encrypt information?

Encryption is in place to mitigate unauthorized access, unauthorized disclosure and loss of business-critical information due to intentional or unintentional causes. Applicable fields of encryption include:

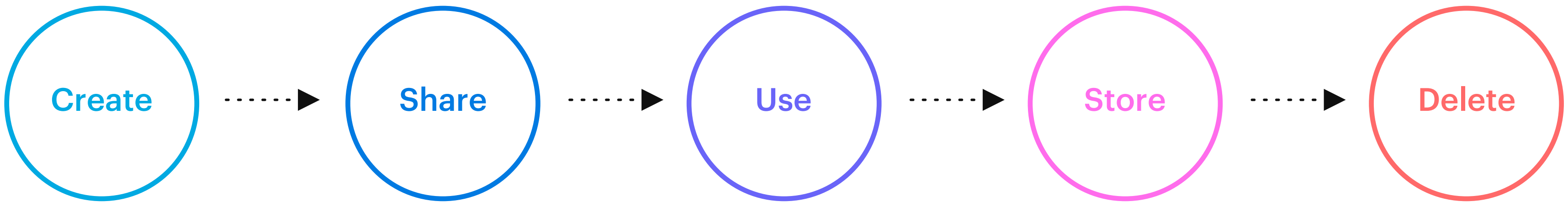
Secure communication between parties	Secure data retention and archiving	Demonstrating data reliability
Preventing others from listening or monitoring communication	Ensuring that data is unaltered and inaccessible while kept at rest	Guaranteeing that data is available in its original untampered format

What information to encrypt?

Any information that holds value for an organization is considered business-critical information that must be encrypted. Generally, business-critical information refers to: Word processor and Text files, Spreadsheet files, Presentation files, Image files, Audio files, Video files, Compressed file extensions, Disc and Media file extensions, and Executable file extensions. Depending on the industry, business critical information can refer to a number of different things.

When to encrypt information?

Information has a so-called “life cycle” which encompasses the point it was created, shared with others, managed and used, stored at some point, and finally after serving no further purpose, deleted. Regardless of what stage in its life cycle information is currently at, encryption should always be used as a security measure.



02

The fundamentals of encryption

When to encrypt information?

Fundamentally, every encryption method uses the same base concept; transforming plaintext into ciphertext with the use of an encryption key.

Plaintext:

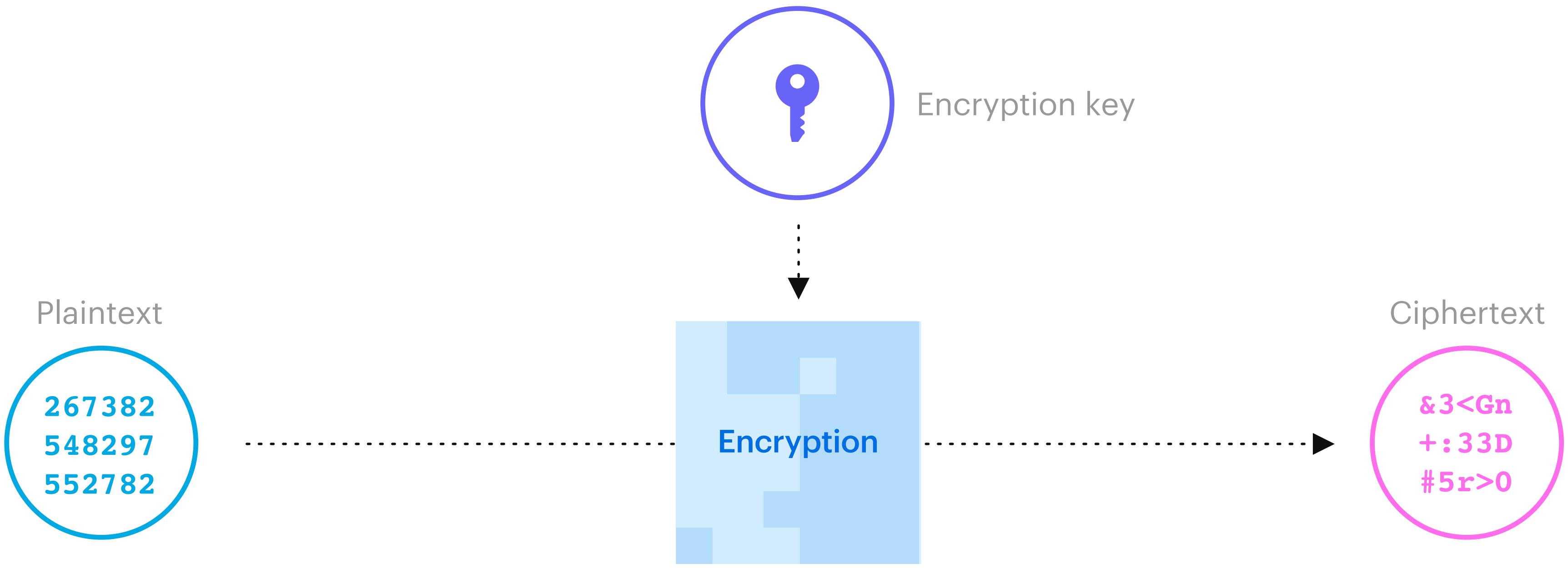
Regardless of its format, before encryption can begin, information must be turned into plaintext. This means it is translated from various formats into a common language that is digestible by the cryptographic algorithm.

Ciphertext:

As a following step, plaintext gets converted into a seemingly random set of numbers, letters and symbols called ciphertext. Ciphertext is the end result of the encryption process.

Encryption key:

In order to turn plaintext into ciphertext, a key is required that contains the rule set of the conversion. The encryption key is responsible for putting logic behind the seemingly random set of characters in the ciphertext.

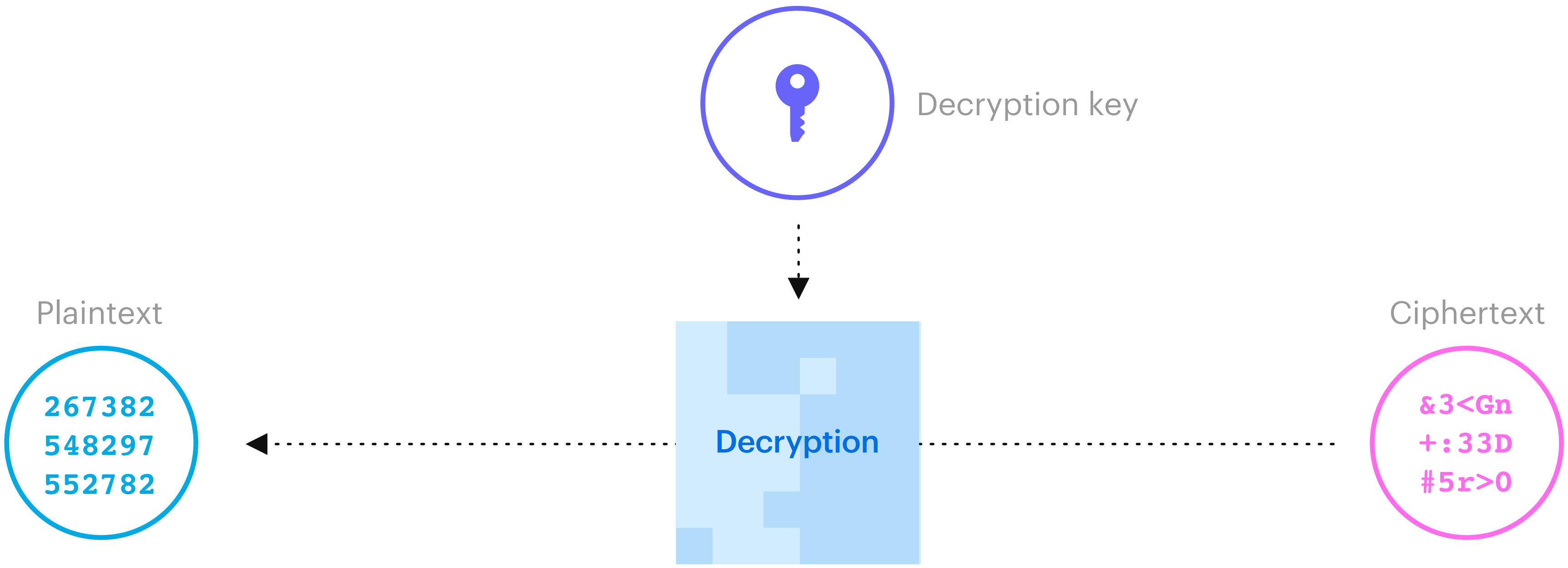


Decryption

Decryption is done by applying the same process as encryption the other way around. Ciphertext is transformed into plaintext with the use of a decryption key.

Decryption key:

The decryption key is not necessarily the same as the encryption key but when created it was based on the same rule set. It is mathematically guaranteed that decryption works only if the decryption key matches the logic of the encryption key. Those in possession of the decryption key are the only parties able to decipher the encrypted information.



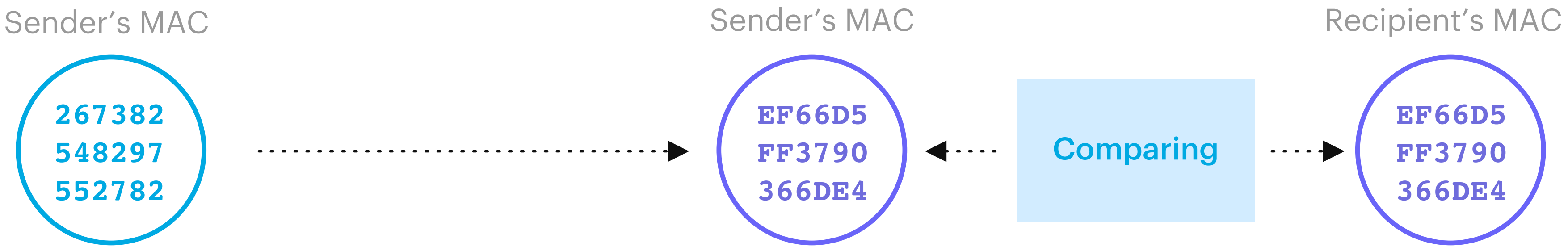
02

Encryption is as good as information reliability

Encryption on its own only focuses on rendering information unreadable to unauthorized parties. In order to guarantee information reliability, a process needs to be in place which makes sure that the encrypted information originates from a legitimate source and not from malicious parties. This process is called a digital signature and consists of two parts: data authentication and verification.

Authentication:
Also referred to as message authentication. It consists of creating a Message Authentication Code (MAC) on the sender side that is delivered along with the encrypted information on a separate communication channel. At the same time, a similar MAC is generated on the recipient side. Once both the encrypted information and the sender's MAC reaches the recipient, verification begins.

Verification:
Comparing the sender's and recipient's MAC. The two keys do not necessarily need to be the same, but they must follow the same mathematical logic. Comparison in this case is based on reconstructing the rule set out of the two MACs. If the end result is the same, the system verifies the transmitted encrypted data and allows it to be decrypted.



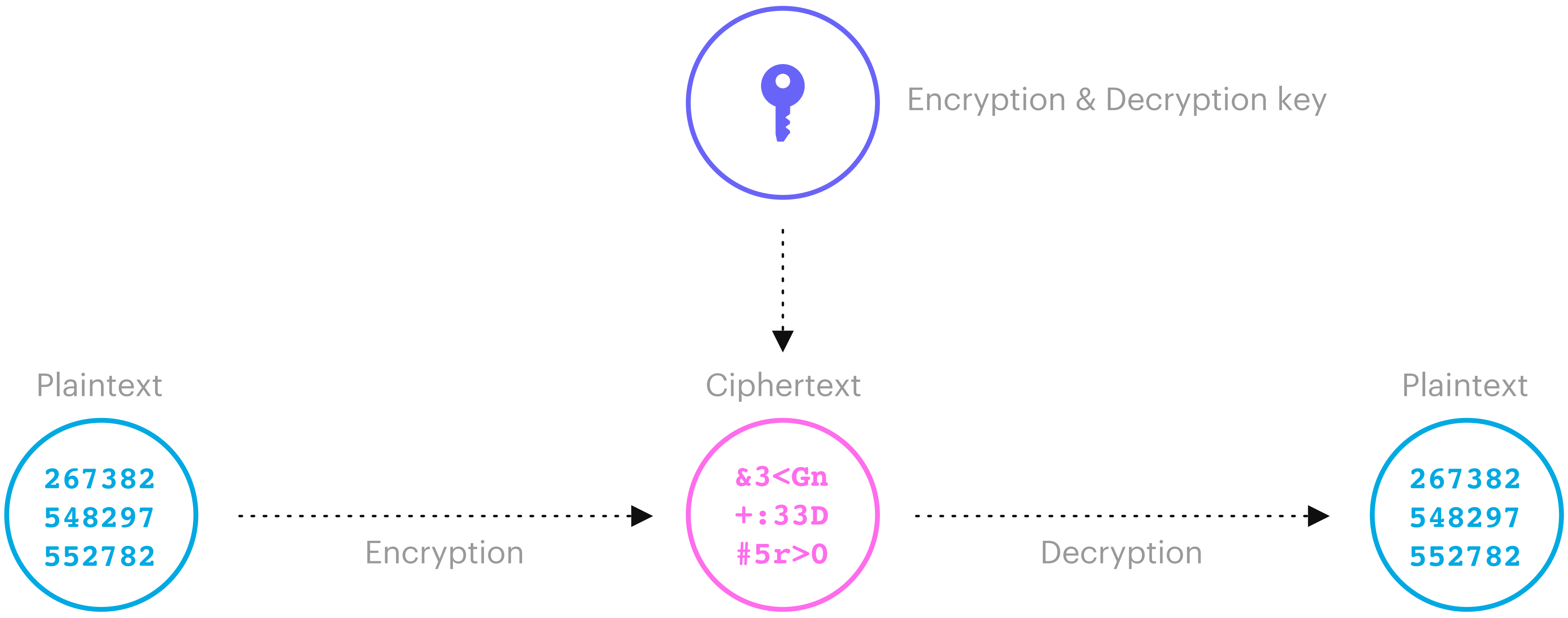
03

Encryption is only as good as the keys

No matter how secure information is thanks to encryption, if the key is disclosed either intentionally or unintentionally, there is no telling who could gain access. Key construction is based on two concepts:

Symmetric keys:

This key constructing algorithm got its name from the fact that the encryption and decryption keys are one and the same. This also applies to the approval process, meaning that the authentication and verification keys are identical too. This means that both the sender and the receiver have to know the key in order to successfully communicate. This poses an additional problem, namely that this key has to be securely shared somehow between the two parties. On the other hand, a symmetric algorithm allows for a fast process, so that large volumes of data can be protected more effectively.



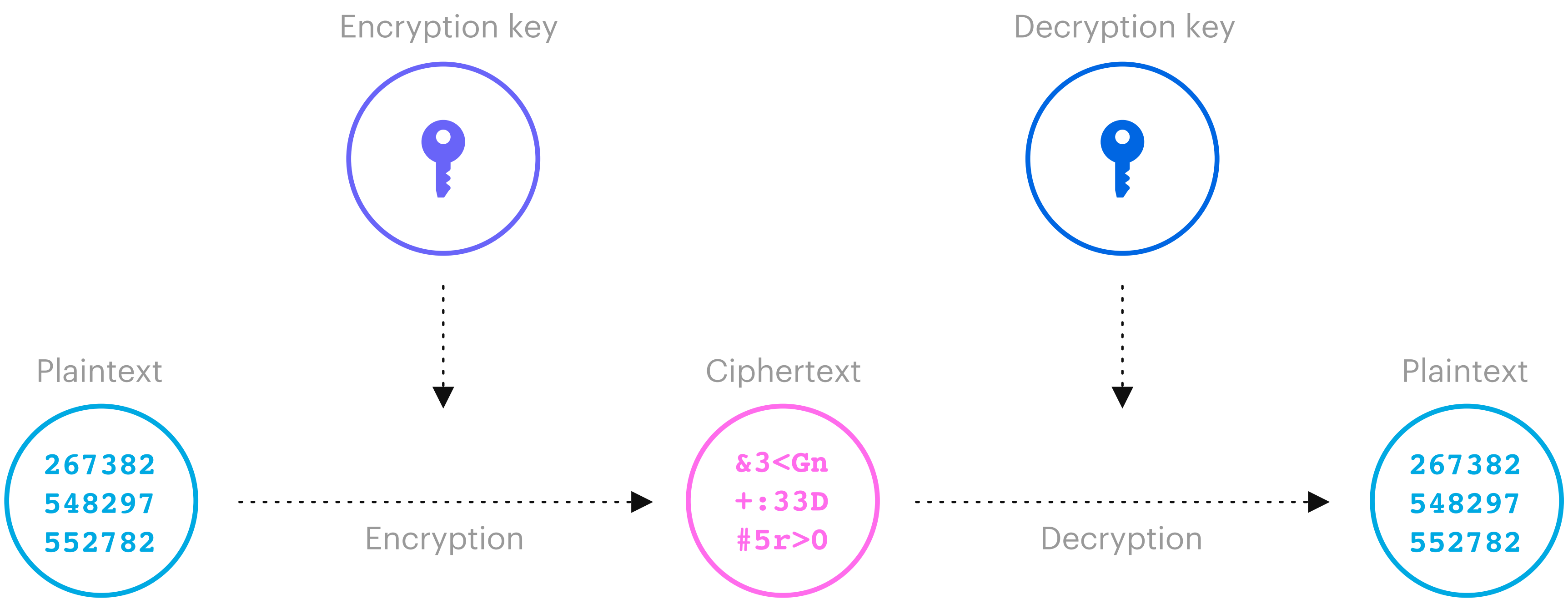
Asymmetric keys:

When using asymmetric or public key cryptography, the encryption and decryption keys are different. One is called public key and the other is called private key.

Public key:
As the name suggests, it is publicly available. Regardless of who knows this key security is not affected. The only thing that needs to be kept secret is the private key.

Private key:
There is a relation between the two keys, but it is mathematically proven that while it is quite simple to calculate the public key from the private one, it would take years to recreate the private key from the public one.

The sender uses the recipient's public key to encrypt the message. This ensures that only the recipient will be able to decrypt it



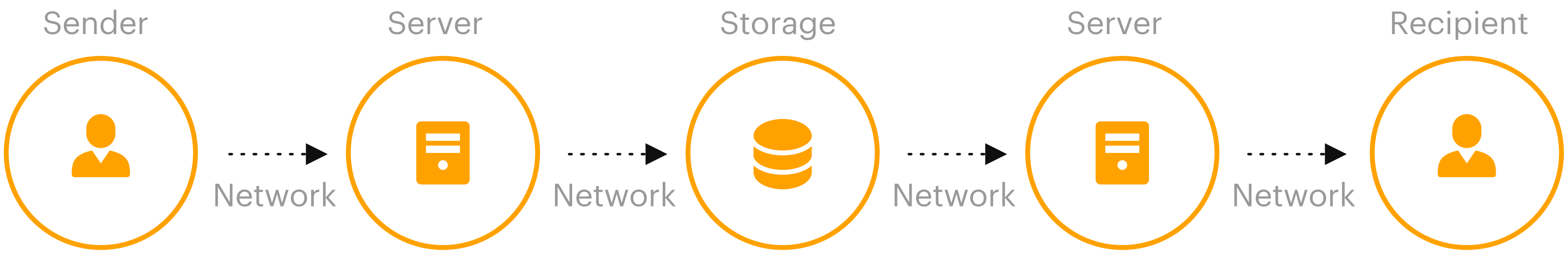
04

Encryption is only as good as the implemented information security processes

By approaching encryption from an information security perspective, we can differentiate based on the information lifecycle stage when encryption is applied.

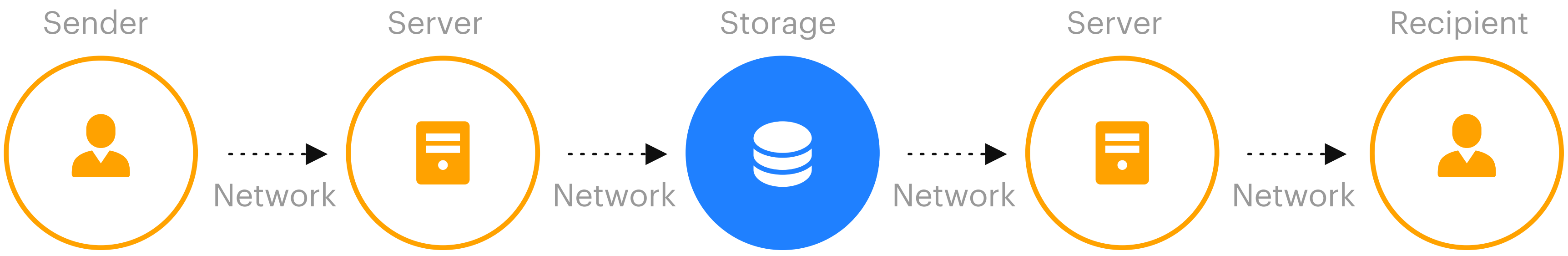
In transit encryption:

The communication channel between the client and the server is encrypted. The purpose of channel encryption is to mitigate eavesdropping on the communication.

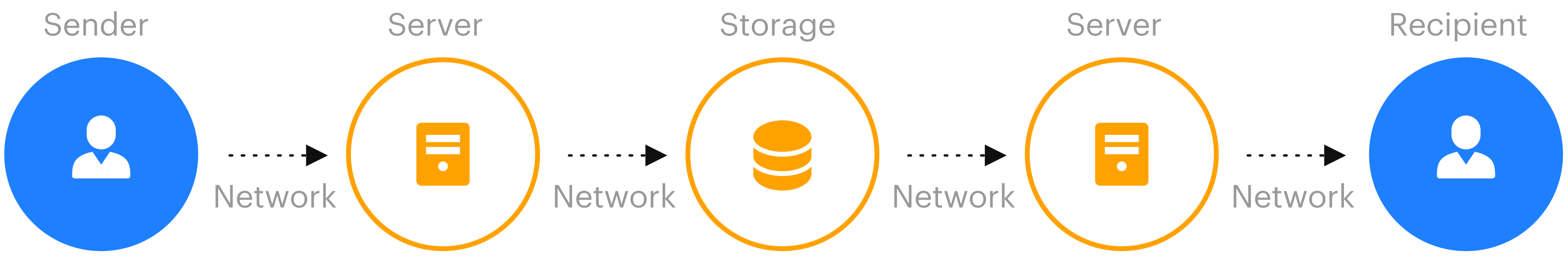


At rest encryption:

Encryption is done at the server-side during storage. At rest encryption adds an extra layer of protection against server-side attackers as the encrypted information and keys are stored separately.



Hardware encryption:
Data encryption happens on the end-point device's hard drive. Hardware encryption is used to protect information on lost or stolen devices by ensuring that all information is stored in encrypted format and only accessible via password authentication.



05

Partial vs constant information security

In the beginning of this paper, a statement was made on the difference between partial and constant information security. All the aspects we covered so far, if used incorrectly or only applied sparsely, will essentially lead to partial information security. In other words, there will be periods when data is unnecessarily decrypted and exposed to malicious intents. In order to ensure information security at all times, all described components must be aligned, which is the fundamental principle of end-to-end encryption.

What is end-to-end encryption?

Everything described to this point about encryption contributes in some way to end-to-end encryption (E2EE). Technologies that provide E2EE are developed by understanding the strengths of each component and turning their weaknesses into benefits. Let's look at each section we touched on from the bottom up and identify how they contribute to E2EE.

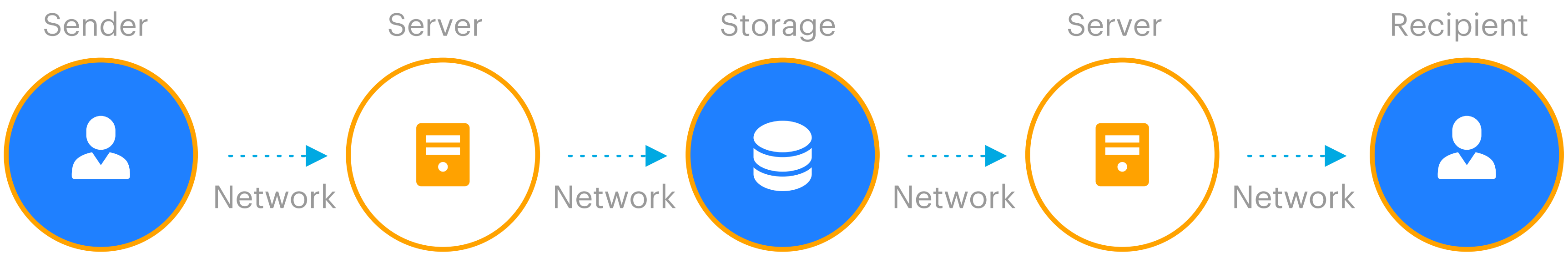
The weaknesses of commonly used information security methods

In transit encryption weaknesses:
The communication channel between the client and the server is encrypted but not the information which travels through, putting it at risk if the transmission is hijacked.

At rest encryption weaknesses:
Encryption is done at the server side for long term storage purposes however once information is in use or in motion again it needs to be decrypted.

Hardware encryption weaknesses: Data encryption happens on the end-point devices to protect information on lost or stolen devices but once information is sent it becomes unencrypted.

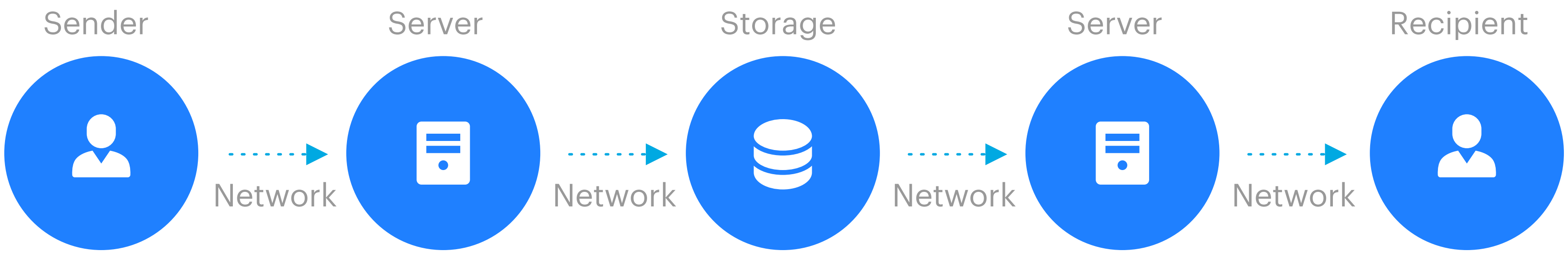
Even if we combine all three, we only get a fairly secure architecture where information is constantly exposed.



Information is unencrypted: before being sent and received, while passing through any channel, once on the server side, right before and after being stored.

Making a difference in information security with end-to-end encryption

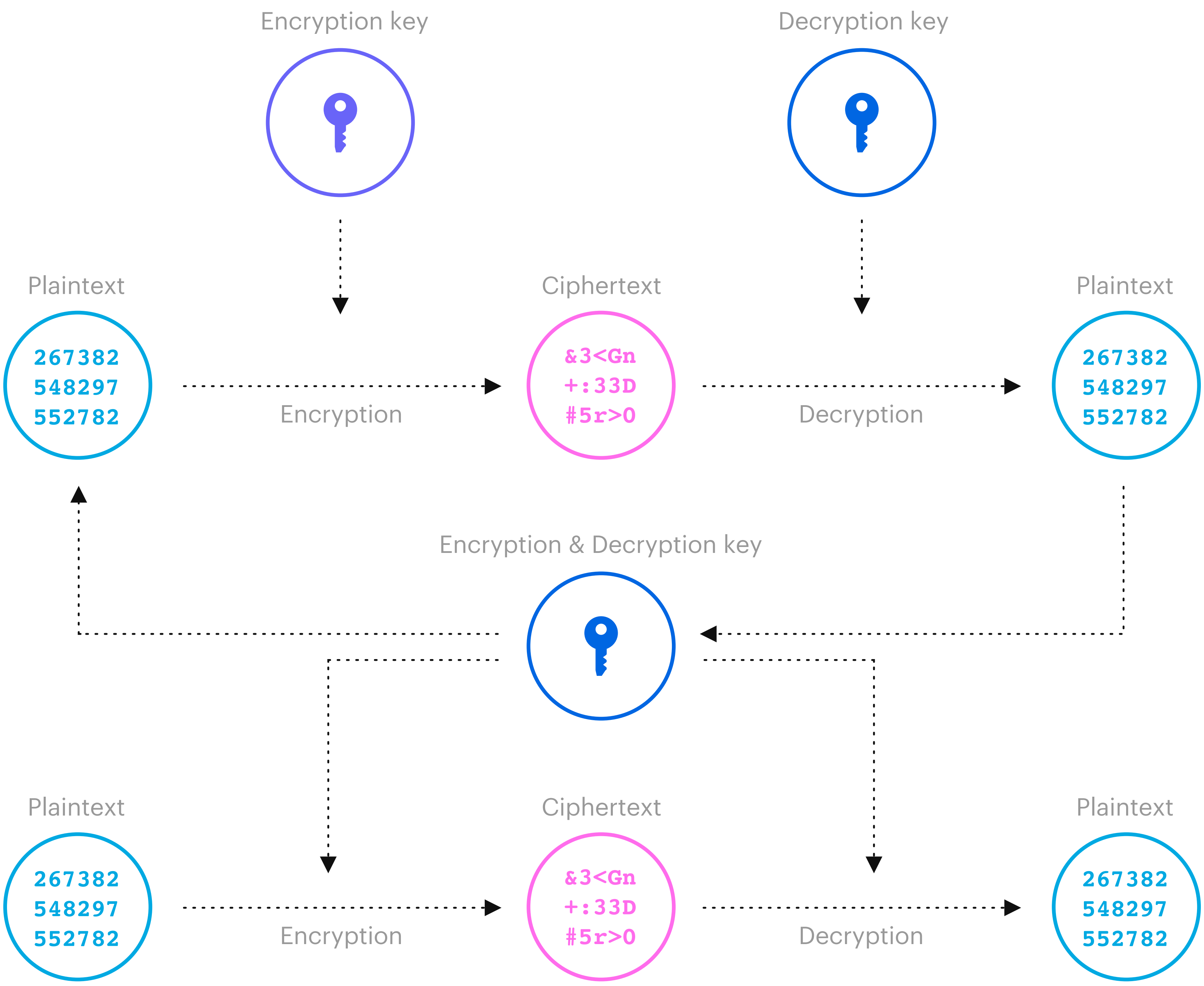
In terms of information security, E2EE starts by introducing client-side encryption. The process of encrypting information on the client side is just like hardware encryption, the difference being that once information is encrypted on the client-side, the same information will be the one that gets transferred and distributed between authorized users. The reason behind it is to ensure that information is only decryptable at endpoints. This way when data is in transit, both the channel and the data itself are encrypted, doubling the security potential and further mitigating any chance of a cyber-attack. During storage the same thing applies - information is still encrypted but also additionally protected on the server. In addition to all of this, E2EE can provide something else that the rest on their own couldn't;
Zero knowledge encryption. This provides an additional layer of insurance that encryption is used properly. Zero knowledge algorithms and protocols prevent information, keys and passwords from being transferred in an unencrypted format.



06

E2EE in key management

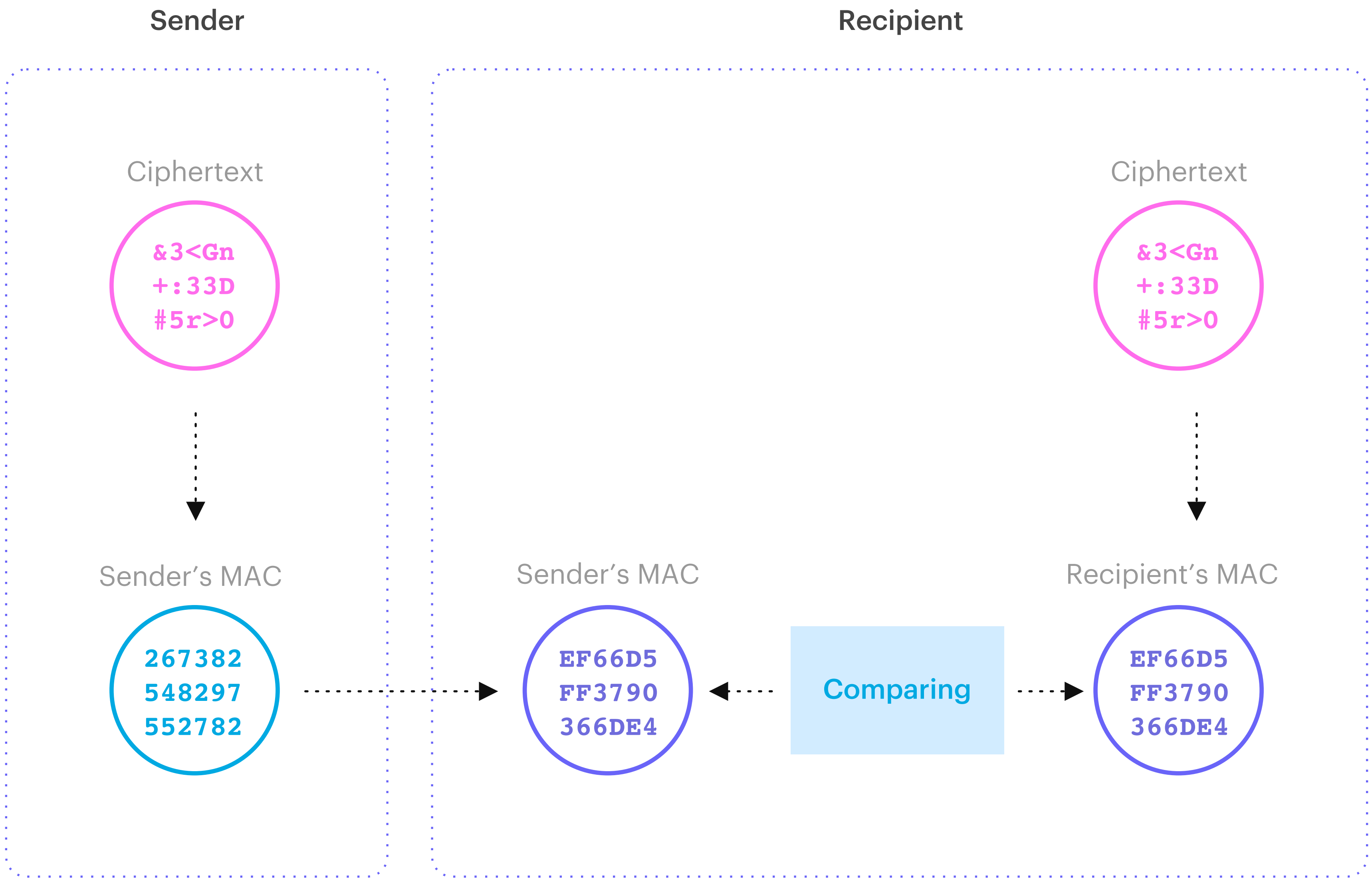
Using asymmetric algorithms, the key distribution problem is solved, as the public key can be shared. The downside is that these algorithms work much slower making it impractical to encrypt and sign more than a few kilobytes of information. End-to-end encryption technologies take both of these factors into consideration and use them to create the best of both worlds. Symmetric keys are used to encrypt information, the keys themselves don’t necessarily take up a lot of space. By allowing asymmetric encryption to be only applied to the keys, the mixing of symmetric and asymmetric encryption provides a highly secure means of protecting information while not consuming too many resources in the process.



07

E2EE in authentication

E2EE technologies combine encryption with authentication to ensure not only that information is secure from malicious elements, but also that it originates from a legitimate source.



08
In conclusion

Aiming for and achieving a highly secure infrastructure is no easy task for any organization but with end-to-end encryption, the safety and security of business-critical information is consistently guaranteed.

09
About Tresorit

Tresorit is the end-to-end encrypted file sync and sharing solution which safeguards confidential information by design for businesses and individuals alike. Trusted by tens of thousands around the globe, our award-winning platform protects sensitive data and ensures compliance with end-to-end encryption. If you wish to learn more about Tresorit or how it guarantees end-to-end encryption and zero-knowledge, visit our website or contact sales.

tresorit

tresorit.com