**Article Editing for** [**https://www.ssl2buy.com/wiki/what-is-encryption-and-decryption**](https://www.ssl2buy.com/wiki/what-is-encryption-and-decryption)

**Keywords:**

* what is encryption
* what is decryption
* encryption vs decryption
* SSL and encryption
* differences between encryption and decryption
* **encrypted vs decrypted**
* what does encryption do
* what does decryption mean

**Titles:**

* **What is Encryption and Decryption in SSL?**
* **Understanding Encryption and Decryption in SSL: A Comprehensive Guide**
* **A Beginner's Guide to Encryption and Decryption in SSL**

**======================================================**

**Introduction:**

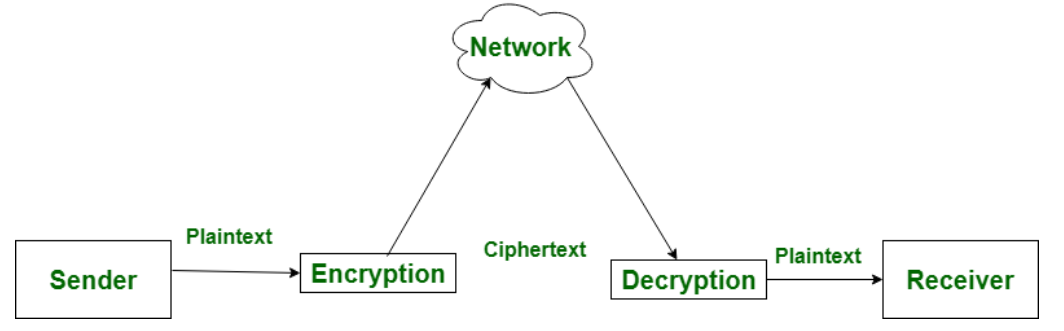
*"****If privacy is outlawed, only outlaws will have privacy****." By Phil Zimmermann (PGP- {Pretty Good Privacy} Creator)*

***"Encryption is the defense against the dark arts in the digital realm."*** *By Edward Snowden, whistleblower*

*These quotes show how vital Encryption is in the digital age. Encryption is not only about watching out for cyber culprits but also about protecting the privacy and freedom of network users throughout the world.*

*Here, two major technologies, titled Encryption and Decryption, have reshaped our thinking about data privacy and security.*

*The concept of Encryption vs. decryption is a pioneer in cryptography, which focuses on data protection by converting it into an indecipherable format and then back into its original form.*



<https://www.geeksforgeeks.org/difference-between-encryption-and-decryption/>

**What is Encryption?**

Encryption is the method of transforming information into a set of characters using algorithms without making it accessible to an unauthorized person. An encrypted message is called a cipher text message. Modern cryptography stands at the crossroads of mathematics and computer sciences. Consider number theory, algebra, computational complexions, fast-paced algorithms, and even quantum mechanisms.

**Growing Threat against SMBs:**

Cyber-attacks on SMBs are on the rise, and they are even more at risk. Data breaches have almost affected small to medium businesses with heavy reputational and financial losses. With the growing threat landscape, Encryption is essential for organizations and individuals. Below are a few statistics related to cyber breaches, which show how crucial data security is nowadays.

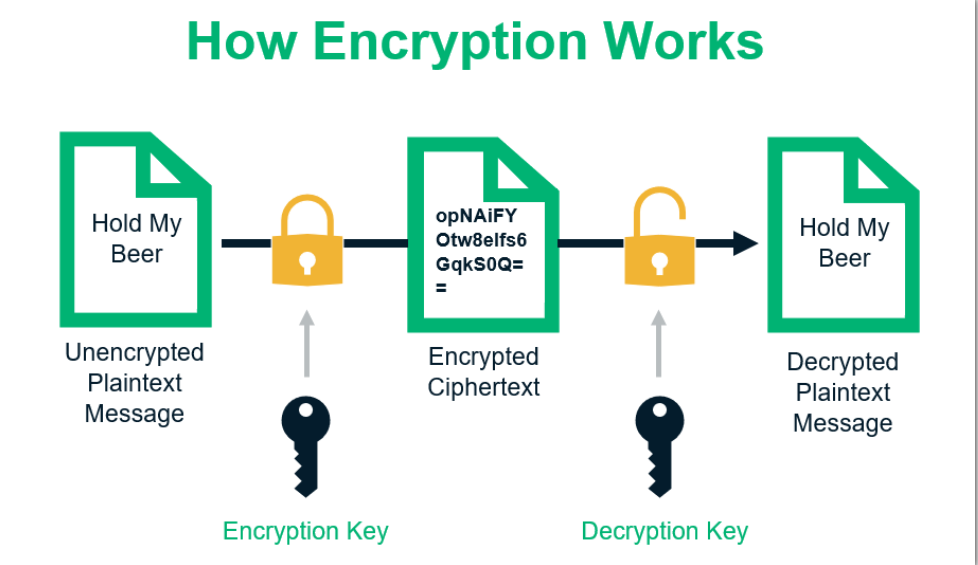


<https://www.pkware.com/blog/data-breach-report-may-2024-edition>

* Nearly 46% cyber breaches affect small companies having less than 1000 employees.
* 75% of SMBs stop their businesses after hitting with ransomware attack.
* 95% of cyber security incidents at SMBs responsible for the cost between $826 and $653,587.

**What Does Encryption Do?**

Encryption is the process of transforming a piece of data or “plain text” to its encrypted form or “cipher text,” generally through cryptographic algorithms. Reverse transformation can be done by decryption key, which is a secret key, a string of numbers, or a password. The higher security added to encryption makes its key size so large that a malicious user has no chance of guessing it.



<https://sectigostore.com/blog/what-is-asymmetric-encryption-how-does-it-work/>

One of the first examples of used cryptography was the “Caesar cipher,” whose namesake was Julius Caesar, who employed it in his private letters. The process is called a substitution cipher, where one character is replaced by another character, which is positioned in a certain number of slots to the right of the replaced character in the English alphabet. To decode the encrypted message, the receiver would know the key to the cipher, which is a shift down the alphabet in four places and to the left (a “left shift four”). Thus, each “E” becomes a “Y” and so on.



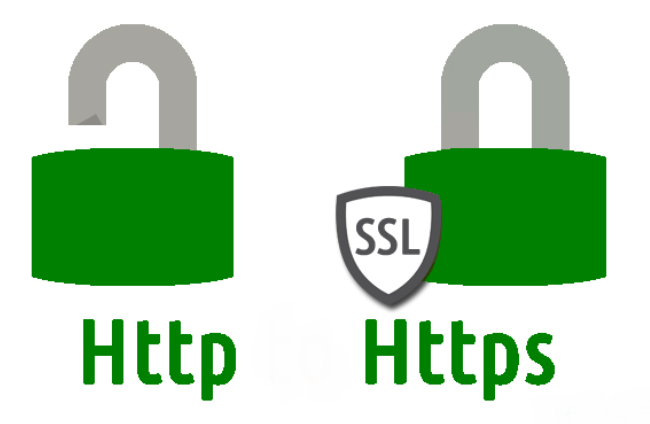
<https://www.sciencedirect.com/topics/computer-science/caesar-cipher#:~:text=The%20Caesar%20cipher%20is%20a,another%20in%20a%20consistent%20fashion.>

The goal of Data Encryption is incomplete without confidentiality, data integrity, identification, non-repudiation and authentication.

* **Data Integrity** refers to accidental or unofficial modification of data. Here, the data receiver needs to verify that the data is not altered.
* **Confidentiality**, where access to data is restricted, and only authorized individuals are allowed to access the data. It prevents the disclosure of information to unauthorized persons.
* **Identification and Authentication** belong to confirmation of originator data transmission. It ensures that the data originated from the actual receiver.
* **Non-repudiation** ensures that the data receiver is known to the sender’s identity. Both the sender and receiver cannot deny their involvement in data transactions.

**How Encryption is correlated with SSL?**

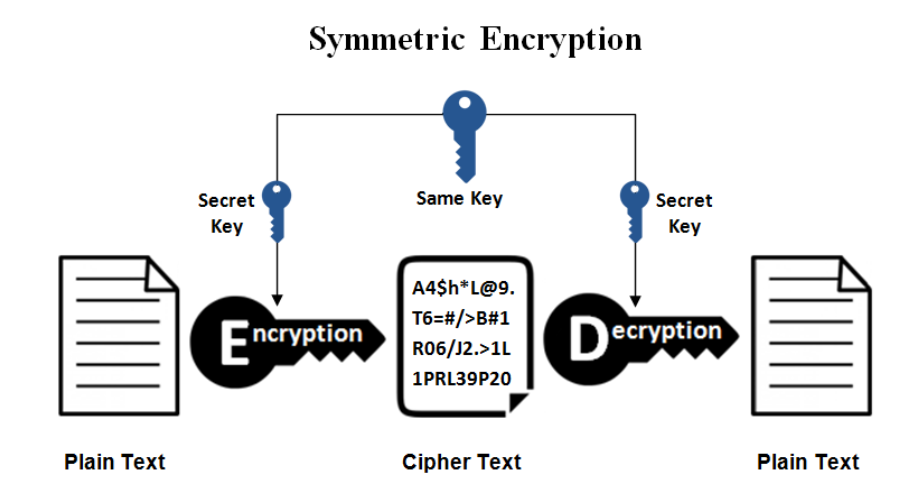
In 1995, the NIST developed SSL, or Secure Socket Layer, a security protocol. SSL and Encryption are related. The main aim of an SSL protocol is to provide data privacy, authenticity, and integrity. SSL is an earlier version of the TLS protocol. A website with SSL enables HTTPS before the domain name, which assures data privacy and security.



<https://www.geeksforgeeks.org/difference-between-http-and-https-2/>

To provide privacy and security, the SSL protocol uses encryption and decryption processes for data transmitted across the web. Encryption works using symmetric and asymmetric encryption methods.

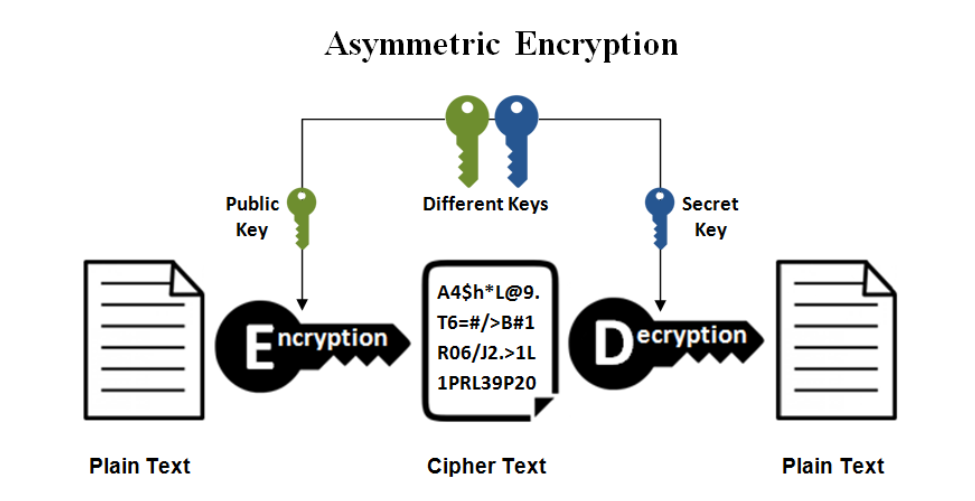
**Symmetric Encryption:** A single key is involved in symmetric encryption to encode and decode the data. This key is also referred to as a secret or private key. Symmetric Encryption is used to preserve confidentiality.



<https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences>

Symmetric Encryption is an ancient process of data security. Typically, it refers to a secret key, which may be a string of random letters, numbers, or words. The sender and receiver mutually possess a confidential key for Encryption and decryption. Symmetric Encryption embraces modern algorithms such as Blowfish, AES, DES, RC5, and RC6, with AES-128, AES-192, and AES-256 being the prevailing encryption standards.

**Asymmetric Encryption:** Asymmetric Encryption mainly works on two keys, a public key and a private key. This encryption system is essential to ensure that online communication, such as sending an encrypted message or checking the digital signature, is safe. With a set of keys, it is easy to communicate with numerous parties, making it more scalable within expansive networks.



<https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences>

In this case, Encryption not only provides private and secure email but also works as the foundation of encrypted connections with protocols such as HTTPS and the validation of digital signatures.

**What is Decryption?**

The process of decryption converts the encoded data back to its original state. During the entire decryption process, the system converts the data and transforms it into text or images that are easy for the reader and the system to understand. The recipients should have access to decrypt the data to get the original text. Decryption can also be performed with software, codes, keys, or passwords. The original file can be in the form of text, images, or directories.

However, the original format is plain text, while the encrypted format is called cipher text. A sender and receiver use algorithms and keys for the encryption and decryption process. The decryption algorithm is called a cipher.

**What Does Decryption Mean?**

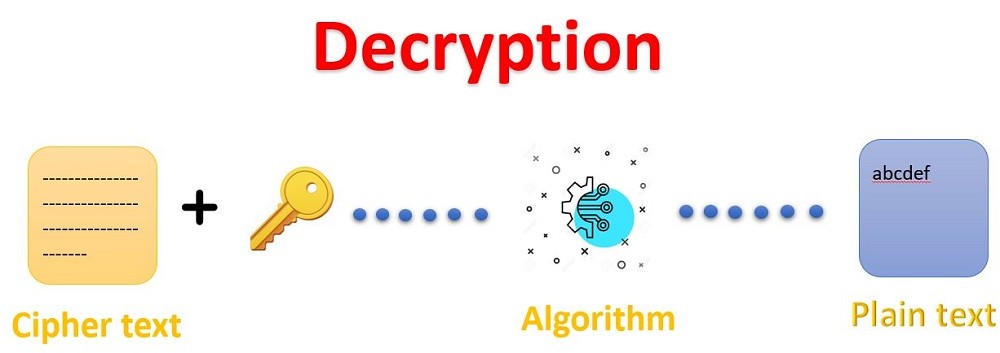
Decryption is essential to safeguard data integrity and data confidentiality, especially when the data is crucial and sensitive. It should be protected from unauthorized persons. Decryption is a core component of cryptography and cyber security. Triple DES, RSA, Blowfish, and AES are standard decryption algorithms.

Below are a few important explanations for the usage of decryption:

* It aids in protecting sensitive data such as login details, including usernames and passwords.
* It ensures privacy for personal information.
* It assists in guaranteeing that the record or file stays unaltered.
* It prevents copying and safeguards intellectual property.
* It is advantageous in network communications, such as the Internet, where a hacker can access non-encrypted data.
* It allows individuals to safeguard their information from unauthorized access securely.

**How Does Decryption Work?**

When we send a private message over the internet, before it is sent over the internet, you encrypt the message using a unique key and thereby turn it into a jumble of characters.



<https://www.linkedin.com/pulse/how-decryption-works-anand-kumar>

At this point, you are the only one who can understand your message. Once the receiver receives the jumbled message, they use the decryption key to reverse the process, thus enabling them to get back the original message. It is like a secret language that only the sender and the receiver can understand.

**Difference between Encryption and Decryption:**

It is now essential to have a glimpse of the difference between encryption and decryption.

**Definition:**

* **Encryption converts the information into an incomprehensible format to avoid interference of third party.**
* Decryption restores data to its original state by converting indecipherable data. It allows only authorized persons to decode the information.

**Process:**

* **In asymmetric encryption, the data transmitted between two machines, will be encrypted with a public key.**
* **In decryption, the data receiver transforms the data into original form with a private key.**

**Location:**

* In encryption, the sender sends the data to the destined server.
* In decryption, the receiver receives the data and converts it to original format.

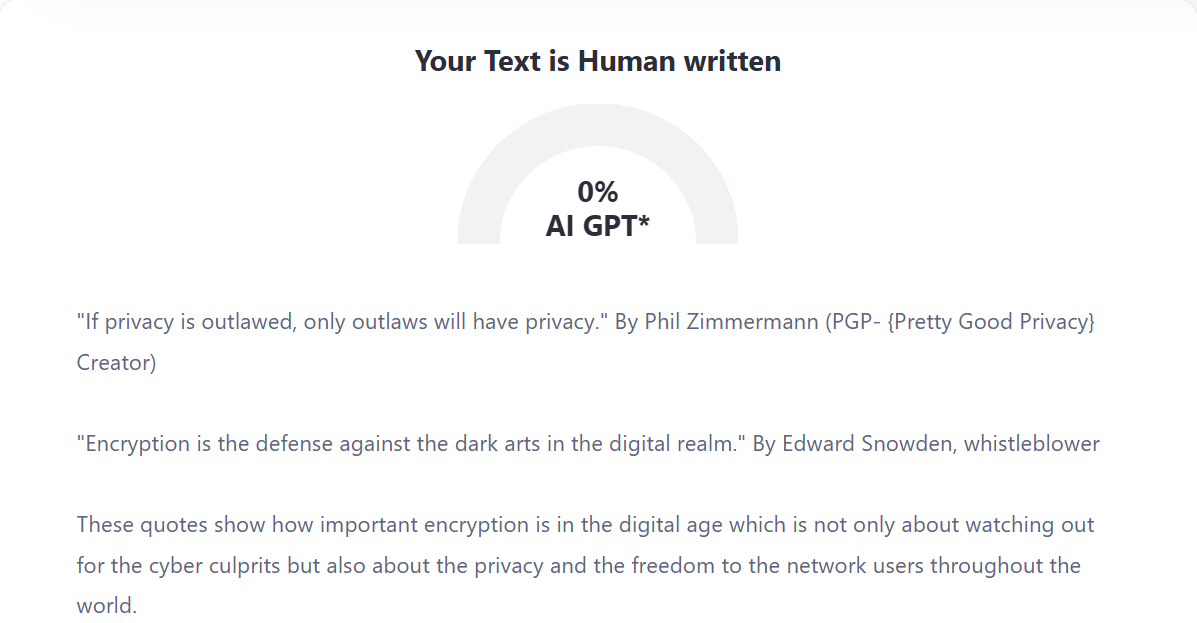
**Use of Algorithm:**

* **A single algorithm and key are used in encryption and decryption process.**
* **A single algorithm is used to encode and decode data but uses two keys for encryption and Decryption.**

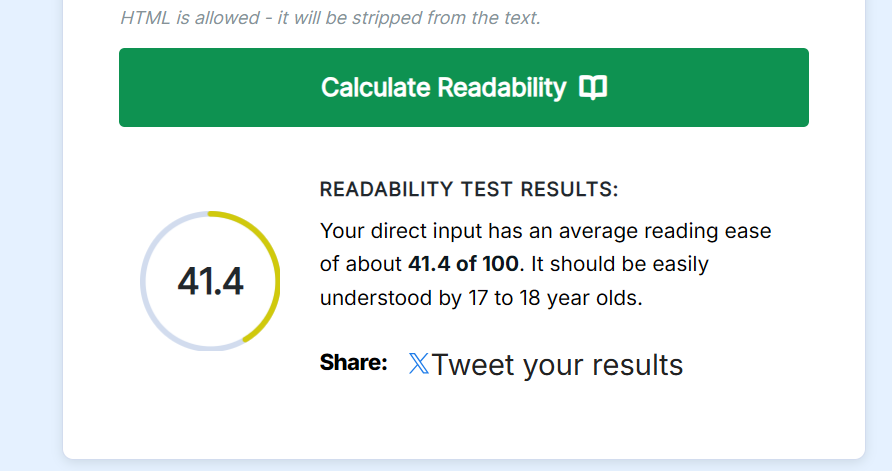
**Primary Function:**

* **Encryption converts plain text into incomprehensible format.**
* **Decryption process converts incomprehensible information into comprehensible format.**

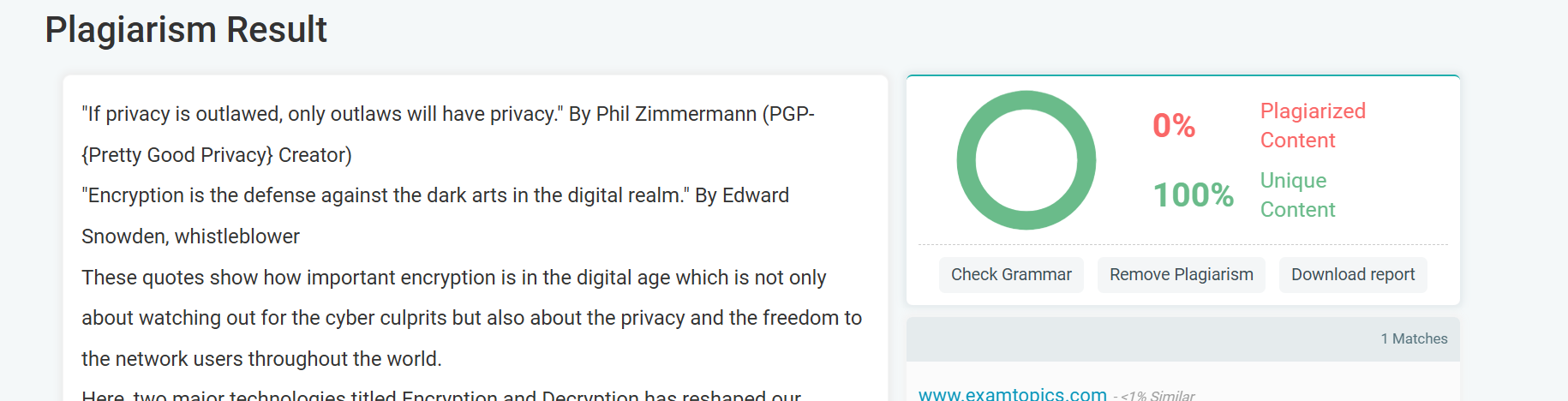
**Conclusion:** As we have seen in this piece of information, there are two main parts to cryptography: encryption and decryption. Both methods use mathematical algorithms to convert data. A secret key known only to the sender and receiver is notably used for secure communication. This secret key is typically a string of characters or a passphrase generated by an algorithm.



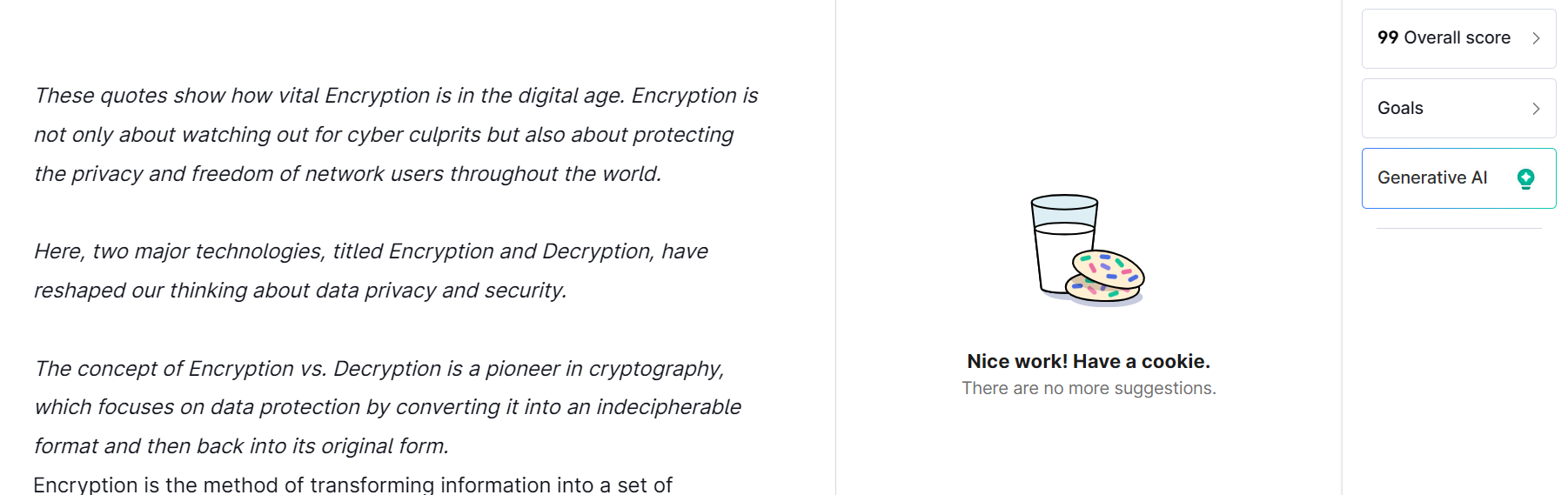
[Source](zerogpt.com)



[Source](webfx.com/tools/read-able/)



[Source](prepostseo.com/plagiarism-checker)



Grammarly.com