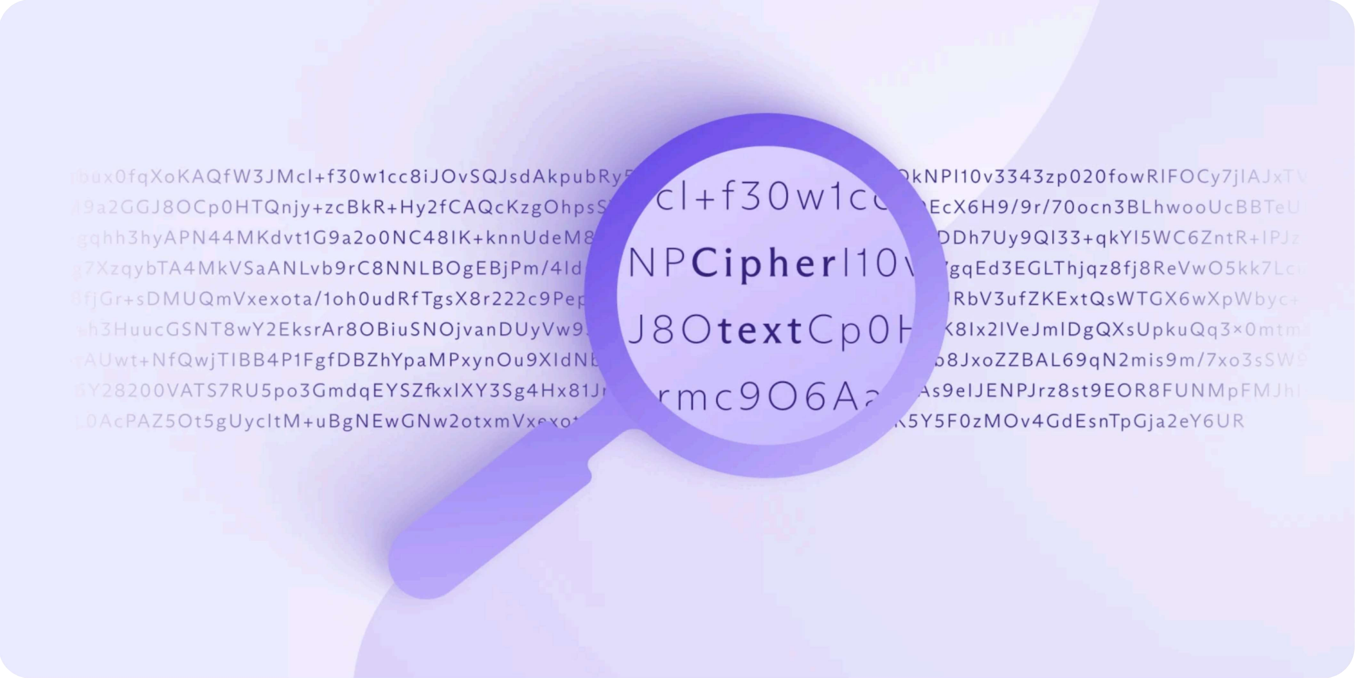


PRIVACY BASICS

What is ciphertext?

Harry Bone

Share

Last update on August 16, 2023 Published on February 24, 2023

Ciphertext is unreadable, encrypted data that can only be read if you know the key. Learn all about ciphertext and how it ensures your data privacy by securing computers and online communications, including encrypted email.

the letters into ciphertext – garbled text that could only be deciphered with a secret key. Only the troops that knew the key could read it.

Two thousand years later, computer-generated ciphertext keeps your confidential data private on your devices and online. We explain what ciphertext is and how it's used to secure online communications, including encrypted email.

What are ciphertext and plaintext?

In cryptography, ciphertext, also known as encrypted text, is the unreadable text that results when you encrypt text.

In contrast, **plaintext** is ordinary, readable text that is not encrypted.

When you encrypt a message using an encryption algorithm known as a **cipher**, your original text (**plaintext**) is transformed into a series of random numbers and letters (**ciphertext**) that can't be read.

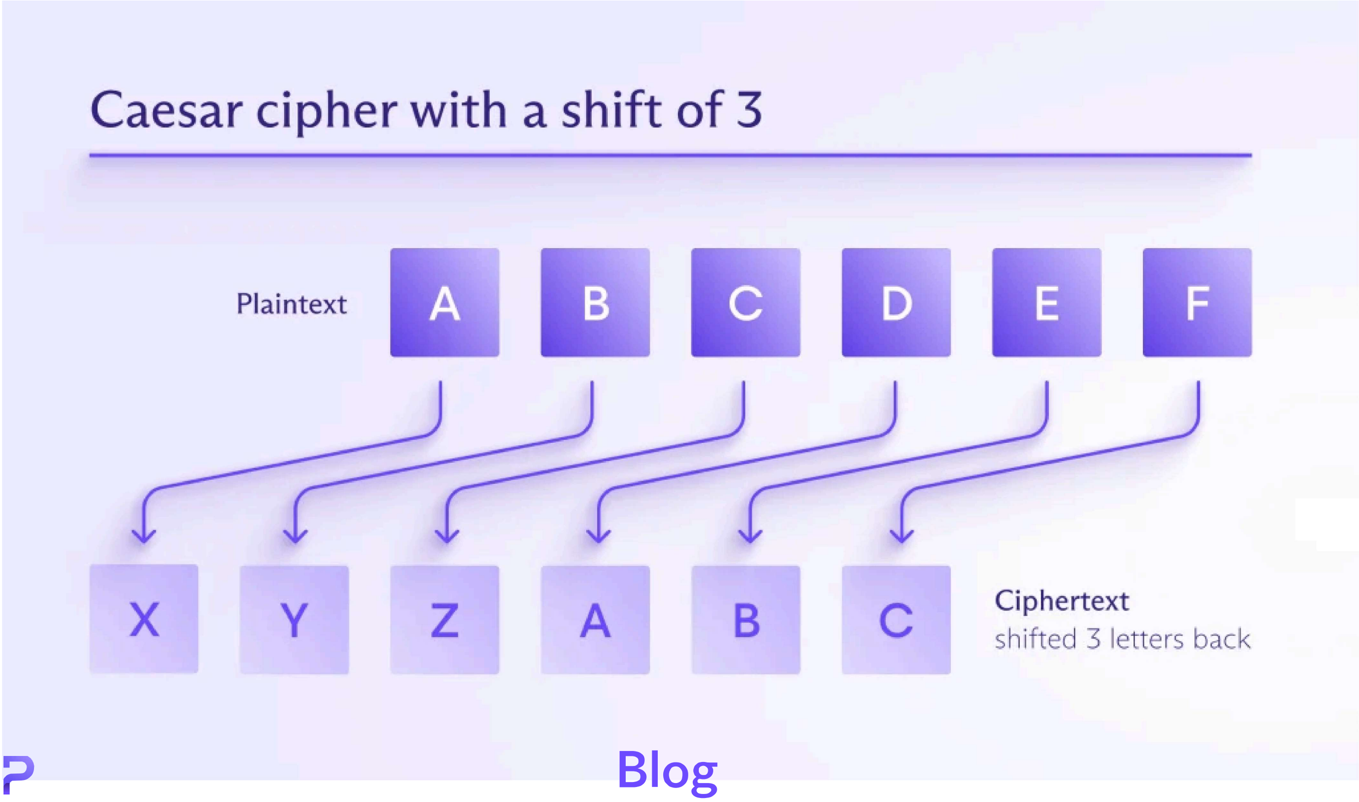
Ciphertext example

Here is some simple ciphertext encrypted using the Caesar cipher, Julius Caesar's original method, which uses letters only:

JV PBZOBQ QBUQ

To encrypt the original message into the ciphertext above, each letter of the text was shifted **three letters back** in the alphabet.

- "A" shifts three letters back and becomes "X"
- "B" becomes "Y"
- "C" becomes "Z"
- and so on…



So to decrypt the message into readable plaintext, you must shift each letter **three letters forward** in the alphabet.

Ciphertext	J	V	P	B	Z	O	B	Q	Q
Plaintext (3 letters forward)	M	Y	S	E	C	R	E	T	T

Deciphering ciphertext into plaintext

So “JV PBZOBQ QBUQ” reads “MY SECRET TEXT”.

In this case, the **key** to the cipher is **3**: you shift each letter three places back or forward in the alphabet to encrypt or decrypt it. This is known as a substitution cipher.

Types of ciphers

Historically, encryption was done by hand, typically using pen and paper. Before the advent of machines, ciphertext was usually created by simply replacing letters (substitution cipher) or re-ordering them (transposition cipher).

These simple ciphers are no longer used as methods of encryption on their own because they’re quite easy to decipher. Today, computer-implemented ciphers are much more secure with long, complex keys consisting of numbers and letters. The longer the key, the harder the cipher is to crack.

handle keys:

1. Asymmetric-key ciphers

Also known as **public-key ciphers**, asymmetric-key ciphers use pairs of mathematically related keys: a **public key** and a **private key**.

You encrypt a message to create ciphertext with a person’s **public key**, which is publicly available and anyone can use. But only that person can decrypt the message into plaintext using their corresponding **private key**, which they keep secret.

2. Symmetric-key ciphers

Also known as **private-key ciphers**, symmetric-key ciphers use a **single key** to encrypt and decrypt the message.

Key type	Key(s)	Examples
Asymmetric-key cipher	Public key Private key	RSA, ECC
Symmetric-key cipher	Single key	AES, ChaCha20, Salsa20

Types of ciphers

Uses of ciphertext

computers and computer networks.

For example, most websites use HTTPS to secure communications, which relies on the TLS encryption protocol. Connect to your bank or an online store, and TLS converts the data you exchange into ciphertext. TLS uses a combination of asymmetric-key and symmetric-key ciphers to secure your connection.

If you connect to the internet using a virtual private network (VPN), like Proton VPN, your internet traffic is transformed into ciphertext using symmetric-key encryption. Proton VPN uses strong AES-256 or ChaCha20 ciphers.

Secure email providers, like Proton Mail, also use encryption to scramble your messages into ciphertext. For Proton Mail, we use AES-256 and ECC or RSA ciphers to implement end-to-end encryption, so only you can read your emails.

Get Proton Mail for free

But with most other email providers that claim to be secure, you can’t guarantee your messages will remain encrypted all the time.

Email ciphertext

Most big email services, like Gmail and Outlook, encrypt emails in two ways. They use:

- **TLS encryption** to secure emails in transit, turning them into ciphertext when they’re being sent from A to B (if the recipient’s server supports TLS)
- **Symmetric-key encryption**, like AES, to encrypt emails stored on their servers

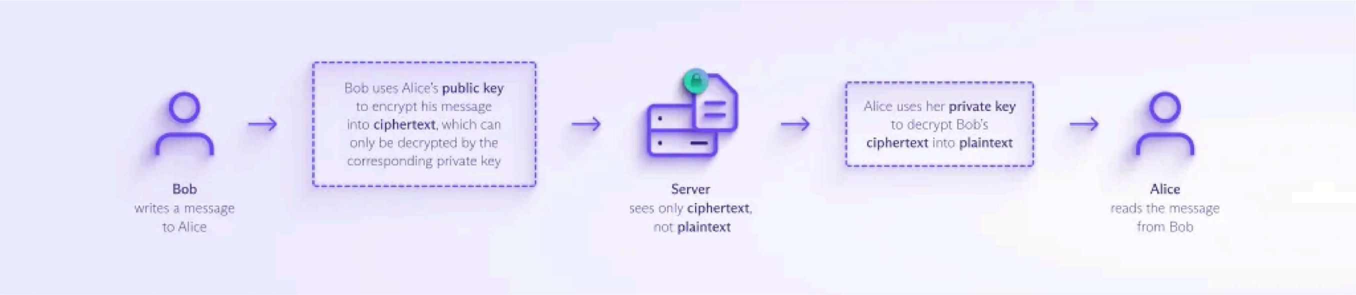
However, who can decrypt your emails remains beyond your control.

"with TLS, the message might not stay encrypted after the message reaches the recipient's email provider".

Second, most email providers retain the encryption keys to your messages. So they can access your data and hand it over to third parties, like advertisers, data brokers, or governments.

The only way to be sure an email you send will remain as ciphertext until your recipient opens it is to use end-to-end encrypted email, like Proton Mail. With end-to-end encryption, your emails are encrypted on your device before being uploaded to our servers and can only be decrypted and read by the intended recipient.

For example, when Bob writes to Alice, his message is converted into ciphertext using Alice's **public key**. Only Alice can decrypt the message into plaintext by using her **private key.**



Bob writes a message to Alice

Bob uses Alice's **public key** to encrypt his message into **ciphertext**, which can only be decrypted by the corresponding private key

Server sees only **ciphertext**, not **plaintext**

Alice uses her **private key** to decrypt Bob's **ciphertext** into **plaintext**

Alice reads the message from Bob

We've designed Proton Mail so that you remain in control of your encryption keys at all times, so only you can access your emails. With Proton Mail you get:

- End-to-end encryption: Any message you send to someone on Proton Mail is end-to-end encrypted by default. No one but you and your intended recipient(s) can read them.

- Zero-access encryption: No one can access any of your stored emails without your authorization, not even Proton.

At Proton, our goal is to keep everyone private and secure online, so join us. With Proton Mail, you decide who can decipher your encrypted emails, attachments, contacts, and calendar.

Share

Harry Bone

A long-standing privacy advocate, Harry worked as a translator and writer in a range of industries, including a stint in Moscow monitoring the Russian media for the BBC. He joined Proton to promote privacy, security, and freedom for everyone online.

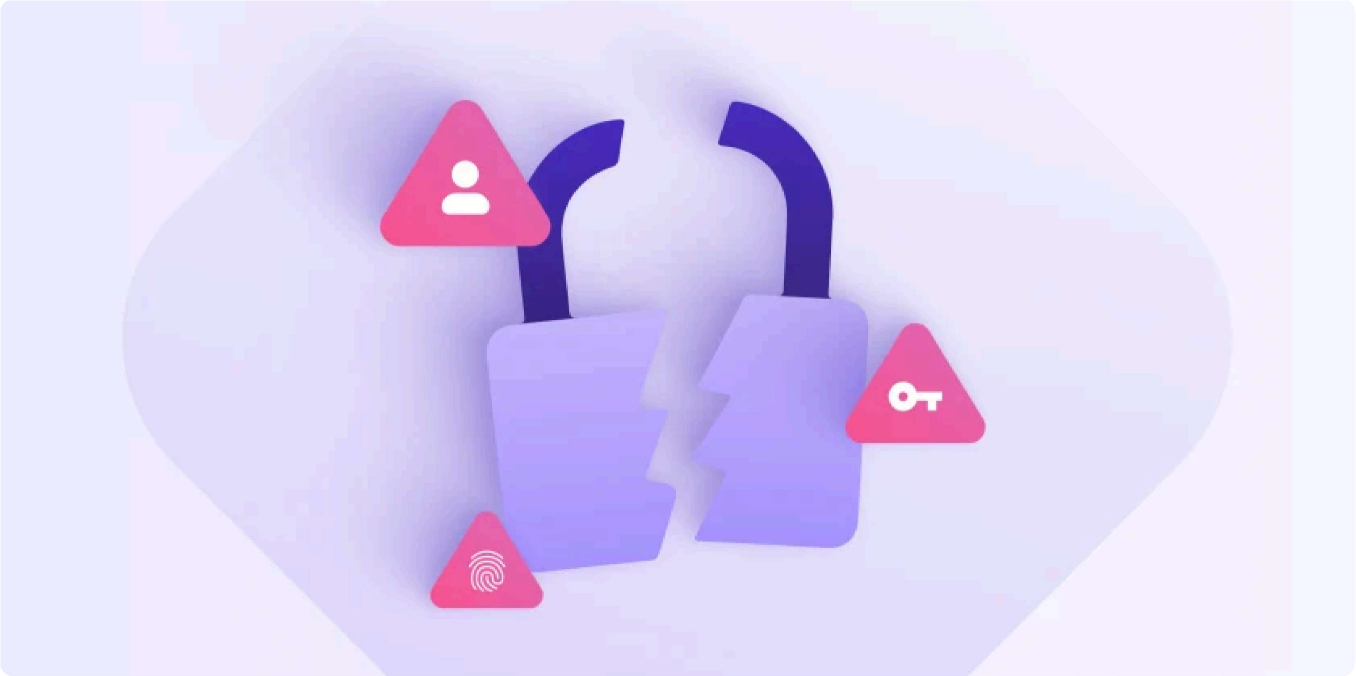
Related articles

Blog

PRIVACY BASICS

What to do if someone has your Social Security number

If you’re a United States citizen or permanent resident, you have a Social Security number (SSN). This number is the linchpin of much of your existence, linked to…



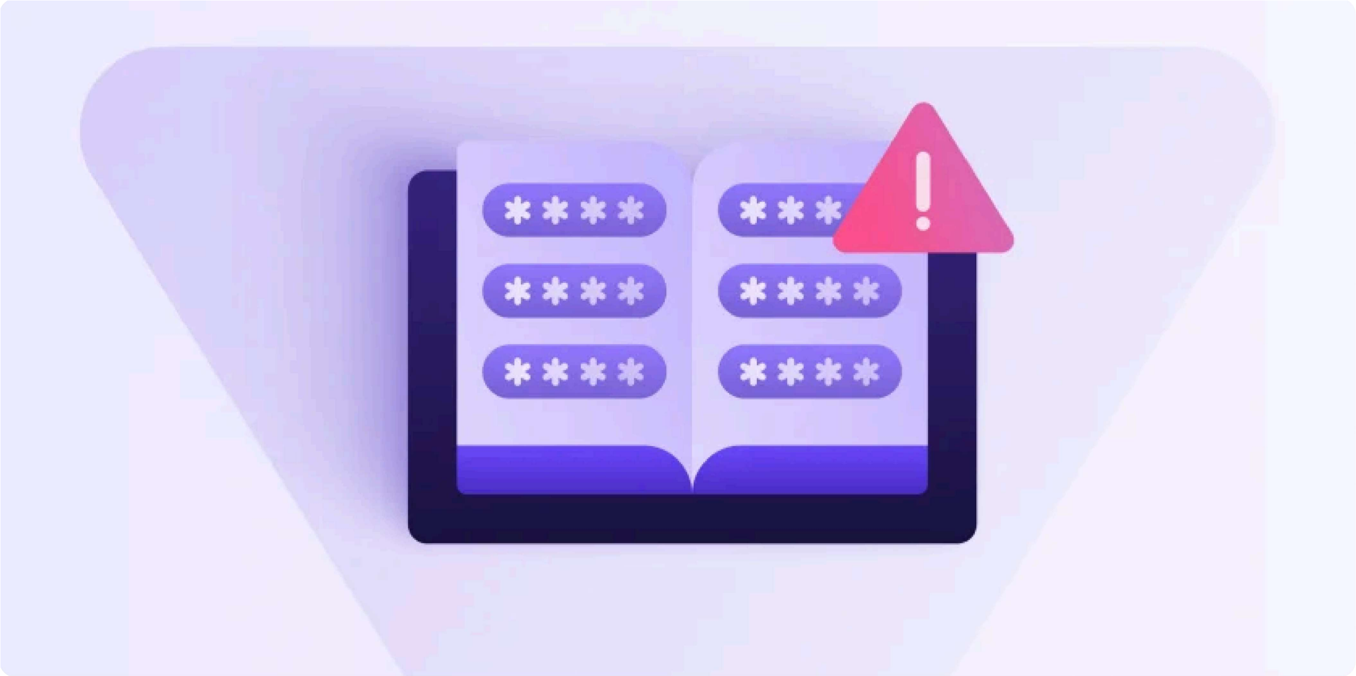
PRIVACY BASICS

How do passwords become compromised?

PRIVACY BASICS

Is WeTransfer safe?

WeTransfer is a popular service used by millions worldwide to send large files. You may have wondered if it’s safe or whether you should use it to share sensitive files. We…



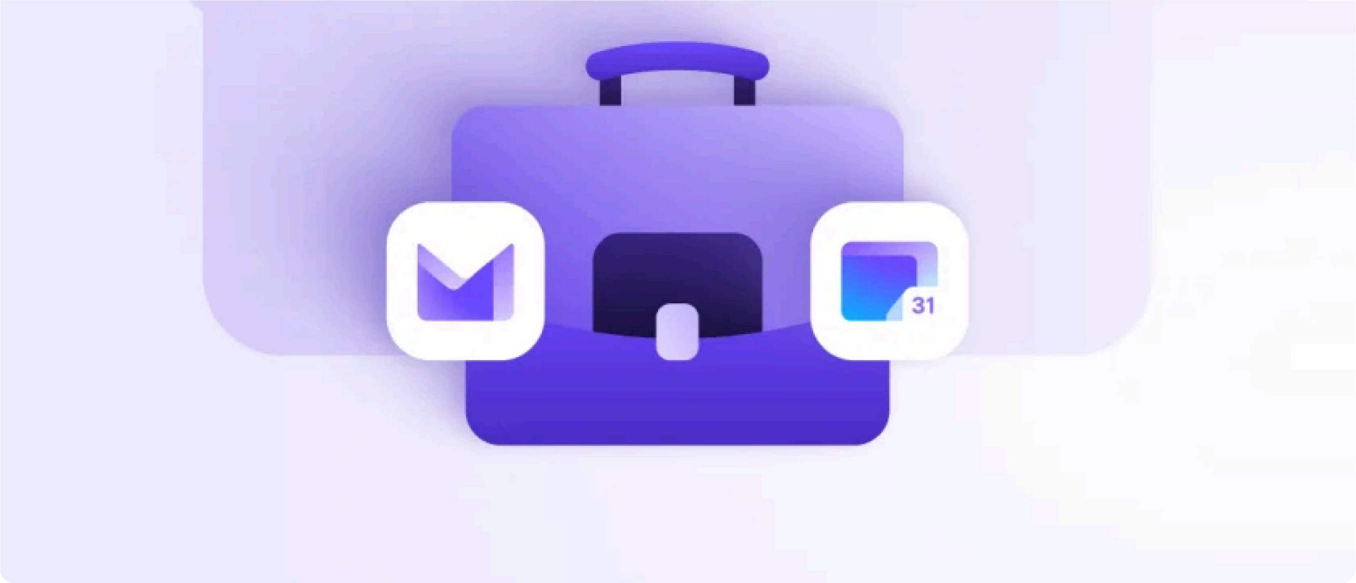
PRIVACY BASICS

Dictionary attacks are a common method hackers use to try to crack passwords and break into online accounts. While these attacks may be effective against people with...

PROTON NEWS

Proton Pass introduces enhanced identity protection with Pass Monitor

Data breaches are increasingly common. Whenever you sign up for an online service, you provide it with personal information that's valuable to hackers, such as email...



FOR BUSINESS

Introducing seamless productivity features for Proton Mail and Proton Calendar

Secure, seamless communication is the foundation of every business. As more organizations secure their data with Proton, we've dramatically expanded our…

Proton - Privacy by default

Proton news Privacy news Privacy basics Privacy deep dives Opinion For busine

Swiss Confederation
Innosuisse - Swiss Innovation Agency

System status Report abuse Report a problem Report a security issue Request a feature

Privacy policy | Terms & conditions | Transparency report |