What Is Cryptography?

Cryptography is the art of locking a secret so only the right person can open it — from Caesar's cipher to modern codes.

Introduction

Long before computers, kings and generals needed to send secret orders. If the enemy caught the messenger, the message had to look like nonsense. So they scrambled the letters — and only the receiver knew how to unscramble them. That scrambling is cryptography, and it is over 2,000 years old.

Cryptography has two jobs: **encryption** (locking a message) and **decryption** (opening it again). The lock is made by a **cipher** (the method) and a **key** (the secret that makes this lock different from every other lock). Without the key, even someone who knows the method cannot read the message.

Today the same idea protects your WhatsApp chats, your bank login, and your exam portal. The ciphers are stronger and the keys are longer, but the idea is exactly the same as Caesar's.

In this lesson you will scramble a message yourself with the Caesar cipher, learn the words cipher, key, plaintext and ciphertext, and see why a long key and a good method both matter.

(Roman Urdu: Cryptography raaz ko band karne ka fun hai — message aisa likho ke sirf wohi parh sake jiske paas chabi (key) ho. Caesar ka cipher iski sab se purani misaal hai.)

A common beginner mistake: hiding a message is not the same as encrypting it. Writing in tiny font, or in a language the reader does not know, is hiding — anyone who looks closely still reads it. Encryption changes the message itself, so looking closely does not help.

Key points

- **Plaintext is the readable message; ciphertext is the scrambled message.** Encryption turns plaintext into ciphertext; decryption turns it back.
- **A cipher is the method; a key is the secret.** The method can be public — the key must stay secret. This is Kerckhoffs's principle: a system must stay safe even if the enemy knows how it works, as long as the key is secret.
- **The Caesar cipher shifts each letter by a fixed number.** Shift by 3: A becomes D, B becomes E, and HELLO becomes KHOOR.
- **A key space is all the keys that could exist.** Caesar has only 25 useful keys, so a computer tries them all in a second — that is why it is a toy, not real security.
- **Cryptography gives four services: confidentiality (only the right person reads it), integrity (nobody changed it), authentication (it really came from who it claims), and non-repudiation (the sender cannot later deny sending it).**

- **Cryptanalysis is the attacker's job: breaking codes without the key.** Every cipher in history was eventually broken — and replaced by a stronger one.
- **Modern cryptography uses maths, not letter-shifting.** But the roles are the same: method, key, lock, unlock.

Examples

Example 1 — Caesar cipher by hand (shift 3)

```
Plaintext:  HELLO
Shift each letter 3 forward:
H -> K, E -> H, L -> O, L -> O, O -> R
Ciphertext: KHOOR
```

To decrypt, shift each letter 3 back: KHOOR becomes HELLO again. The key is the number 3. Change the key to 5 and the same message becomes MJQQT.

Example 2 — Caesar cipher in Python (runnable)

```
def caesar(text, shift):
    out = ""
    for ch in text:
        if ch.isalpha():
            base = ord('A') if ch.isupper() else ord('a')
            out += chr((ord(ch) - base + shift) % 26 + base)
        else:
            out += ch
    return out

print(caesar("HELLO", 3))
print(caesar("KHOOR", -3))
```

What you will get:

```
KHOOR
HELLO
```

The same function locks and unlocks — a positive shift locks, a negative shift unlocks. Try shift 13: encrypting twice with 13 returns the original message.

Example 3 — Brute force: why 25 keys is not enough

```
ciphertext = "KHOOR"
for shift in range(1, 26):
    print(shift, caesar(ciphertext, -shift))
```

What you will get (first and last lines):

```
1 JGNNQ
2 IFMMP
3 HELLO
...
25 LIPPS
```

One of the 25 tries prints HELLO — a readable English word. An attacker just reads all 25 lines and picks the one that makes sense. Real ciphers have so many keys that trying them all would take longer than the age of the universe.

Example 4 — Hiding is not encrypting

```
Hiding:      write the password on paper and put it under your mattress.
             Anyone who looks under the mattress reads it.

Encrypting:  turn the password into ciphertext with a key.
             Anyone who finds the ciphertext still cannot read it.
```

Hiding relies on nobody looking. Encrypting relies on maths. Security always prefers maths.

Quick recap

- Plaintext is readable; ciphertext is scrambled; the key decides how.
- A cipher is the method, a key is the secret — the method may be public, the key never.
- Caesar shifts letters; with only 25 keys it falls to brute force in seconds.
- Cryptography gives confidentiality, integrity, authentication, and non-repudiation.
- Hiding a message is not encrypting it.

Common mistakes

1. **Inventing your own cipher** — every home-made code in history was broken quickly by experts. Fix: use ciphers that thousands of experts have tested for years.
2. **Keeping the method secret instead of the key** — once the method leaks, everything breaks. Fix: a public method with a secret key (Kerckhoffs's principle).

3. **Thinking a short key is fine** — a 3-letter password has few combinations; a computer tries them all. Fix: long keys, long passwords.
4. **Confusing encoding with encryption** — Base64 just rewrites data in different letters; anyone can reverse it with no key. Fix: encoding is for transport, encryption is for secrecy.
5. **Encrypting but never checking integrity** — an attacker may not read your message but can still change it in transit. Fix: encryption plus a check that nothing changed (see CS.5).

Practice

1. Encrypt your first name with the Caesar cipher, shift 3, by hand. Then decrypt it back.
2. Run the Python Caesar function above with your own message and shift 7. Then brute-force it with the loop in Example 3 — how many lines until your message appears?
3. Write, in one line each: what is plaintext, what is ciphertext, what is a key?
4. Find one app on your phone that uses encryption (hint: a messaging app that says "end-to-end encrypted"). What would happen if its key leaked?
5. Explain to a friend why Base64 is not encryption: encode the word "secret" in Base64 online and show that anyone can decode it back without a key.

Practice quiz

1. What is the difference between plaintext and ciphertext?

- There is no difference
- Plaintext is readable, ciphertext is scrambled
- Ciphertext is readable, plaintext is scrambled
- Plaintext is encrypted with two keys

Answer: Plaintext is readable, ciphertext is scrambled

2. In the Caesar cipher with shift 3, what does HELLO become?

- HELLO
- KHOOR
- GDKKN
- IFMMP

Answer: KHOOR

3. Why is the Caesar cipher not real security?

- It is too slow
- It has only 25 keys, so anyone can try them all in seconds
- It needs two keys
- It only works on numbers

Answer: It has only 25 keys, so anyone can try them all in seconds

---

Watch the Code Scope channel: https://www.youtube.com/@CodeScopePK — this lesson's own video joins the channel when it is recorded.

Read online: https://scopetreasure.com/notes/cs-what-is-cryptography · More free tools and notes at https://scopetreasure.com