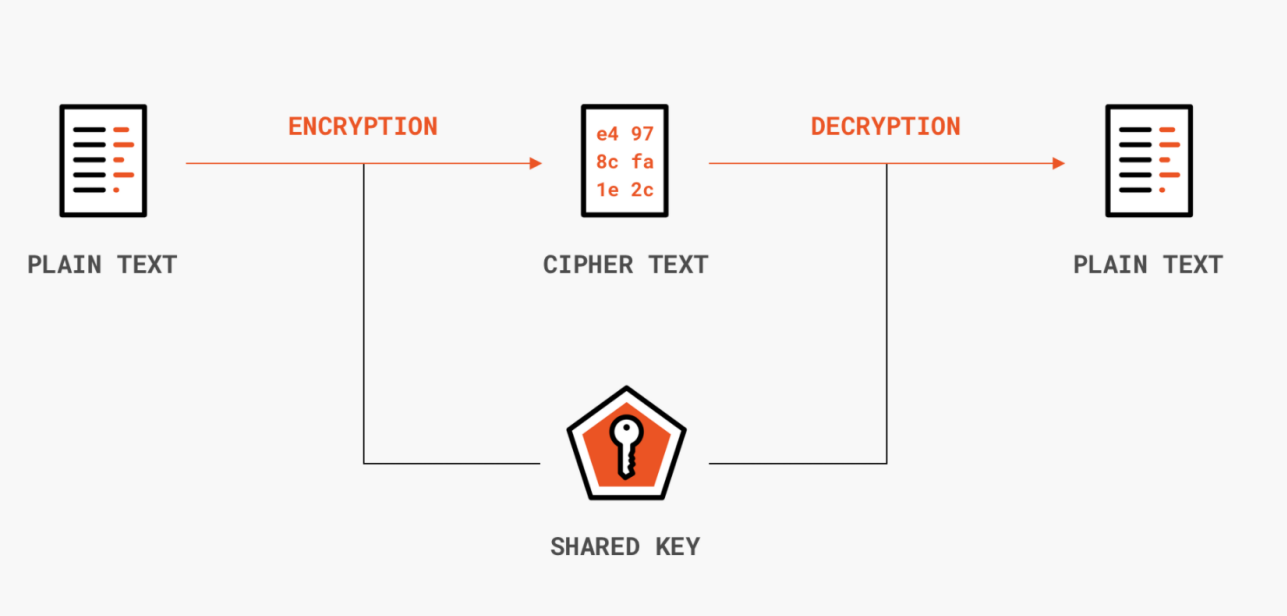
Encriptació

L'encriptació simètrica i l'encriptació asimètrica són els dos tipus principals d'algoritmes utilitzats en la **criptografia** per a assegurar la informació. La diferència clau rau en el nombre de claus que s'utilitzen per xifrar i desxifrar les dades.

Encriptació simètrica (Clau Secreta)

L'encriptació **simètrica** (o de clau secreta) utilitza una **sola clau** per a ambdós processos: xifrar el missatge (convertir-lo en text xifrat) i desxifrar-lo (tornar-lo a convertir en text normal).

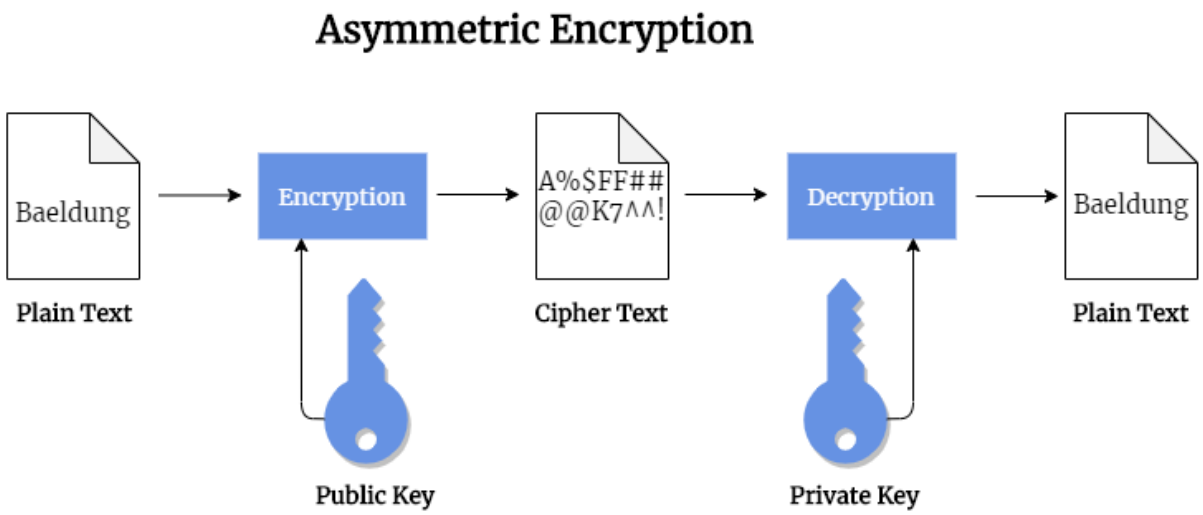
- **Funcionament:** L'emissor i el receptor han de conèixer i compartir la **mateixa clau secreta** abans d'iniciar la comunicació.
- **Avantatges:** És **molt ràpida** i requereix menys recursos computacionals, el que la fa ideal per a xifrar grans volums de dades.
- **Desavantatges:** El principal repte és com compartir de manera segura la clau secreta entre les parts. Si algú intercepta la clau, pot llegir tots els missatges.
- **Exemples:** AES (Advanced Encryption Standard), DES, Triple DES.



Encriptació asimètrica (Clau Pública)

L'encriptació **asimètrica** (o de clau pública) utilitza un **parell de claus** relacionades matemàticament: una de **pública** i una de **privada**.

- **Funcionament:**
  - La **clau pública** es pot compartir lliurement i s'utilitza per a **xifrar** el missatge. Qualsevol pot xifrar, però només el destinatari pot desxifrar.
  - La **clau privada** es manté **secreta** i només la coneix el destinatari, utilitzant-se per a **desxifrar** els missatges.
- **Avantatges:** Soluciona el problema de l'intercanvi de claus. Permet la **confidencialitat** (només el destinatari pot llegir) i l'**autenticació** (amb la signatura digital).
- **Desavantatges:** És **molt més lenta** i intensiva computacionalment que l'encriptació simètrica. S'utilitza per a missatges petits o per intercanviar de forma segura la clau simètrica.
- **Exemples:** RSA, ECC (Elliptic Curve Cryptography), PGP.



Ús combinat

En la pràctica, com en els protocols SSL/TLS (utilitzats en HTTPS), sovint s'utilitza un **enfocament híbrid**:

1. Es fa servir l'encriptació **asimètrica** (més lenta) per intercanviar de forma segura una **clau simètrica**.
2. Després, s'utilitza l'encriptació **simètrica** (més ràpida) per xifrar la gran quantitat de dades de la comunicació.

Característica	Encriptació Simètrica	Encriptació Asimètrica
Claus	1 clau (secreta)	2 claus (pública i privada)
Velocitat	**Més ràpida**	Més lenta
Ús Típic	Xifrat de dades massives, emmagatzematge de dades	Intercanvi segur de claus, signatures digitals, SSL/TLS
Seguretat de la Clau	La clau s'ha de compartir de manera segura	La clau pública es pot compartir; la clau privada ha de ser secreta

Model híbrid: simètric/asimètric en HTTPS

El xifratge de l'HTTPS utilitza un enfocament **híbrid** per combinar la **seguretat** de l'encriptació asimètrica amb la **velocitat** de l'encriptació simètrica. El procés s'anomena "Handshake" (salutació) i funciona així:

Intercanvi segur de clau (Xifratge Asimètric)

Aquesta fase inicial té lloc quan el vostre navegador (client) es connecta al servidor d'una pàgina web:

1. **El servidor envia la seva Clau Pública** (continguda al certificat TLS/SSL) al navegador. Aquesta clau permet al navegador xifrar dades que només el servidor podrà desxifrar.
2. **El navegador genera la Clau Simètrica:** El navegador crea una clau aleatòria (anomenada **clau de sessió**) que s'utilitzarà per xifrar totes les dades posteriors.
3. **El navegador xifra la Clau Simètrica:** El navegador utilitza la **Clau Pública** del servidor per xifrar aquesta clau de sessió simètrica.
4. **El servidor desxifra la Clau Simètrica:** El servidor utilitza la seva **Clau Privada** (que només ell coneix) per desxifrar la clau de sessió simètrica.

> **RESULTAT:** Després d'aquest procés, tant el navegador com el servidor tenen la mateixa clau secreta de sessió (la clau simètrica).

Transmissió dades ràpida (Xifratge Simètric)

Un cop establerta la clau de sessió simètrica, comença la comunicació real:

- Per la seva **velocitat i eficiència**, totes les dades transmeses entre el navegador i el servidor (missatges, imatges, contrasenyes, dades bancàries) s'encripten utilitzant aquesta **Clau Simètrica de Sessió compartida**.
- Això garanteix que, fins i tot si un atacant intercepta les dades, només obtindrà text xifrat, ja que **no disposa de la clau simètrica** (i la clau privada asimètrica mai s'ha transmès).

> S'utilitza el xifratge **asimètric** per a l'intercanvi inicial de secrets de manera segura, i després el xifratge **simètric** per a la comunicació ràpida i massiva de les dades.

Revisió núm. 1
★Admin l’ha creat 2025-10-14 09:23:05 UTC
Admin l’ha actualitzat 2025-10-14 09:28:40 UTC