



Accés remot: Connectant-se de forma segura

L'accés remot permet connectar-se a ordinadors i dispositius a distància de forma segura. És essencial tant per al treball com per a l'oci, permetent recuperar arxius oblidats, administrar servidors o accedir a sistemes empresarials des de qualsevol lloc.



por Paco Galera

Usos i tecnologies d'accés remot



Diversitat d'usos

Des de recuperar arxius fins a administrar servidors i accedir a sistemes empresarials.



Varietat de tecnologies

Des de sistemes de fitxers compartits fins a eines específiques desenvolupades per empreses.



Múltiples dispositius

Accés des de portàtils, telèfons mòbils o connexions fixes d'Internet.



Dispositius domèstics

Control remot de llums, electrodomèstics i altres dispositius de la llar.



Tasques comunes d'accés remot



Control general

Controlar un ordinador des d'un lloc remot, com accedir a un PC personal des d'un cibercafé.



Ús de perifèrics

Utilitzar dispositius connectats a la xarxa, com impressores remotes.



Configuració

Modificar la configuració d'ordinadors remots o instal·lar/desinstal·lar programari.



Assistència

Proporcionar assistència remota a usuaris o supervisar l'ús d'ordinadors.

Tipus d'accés remot

Sessió de treball a la consola

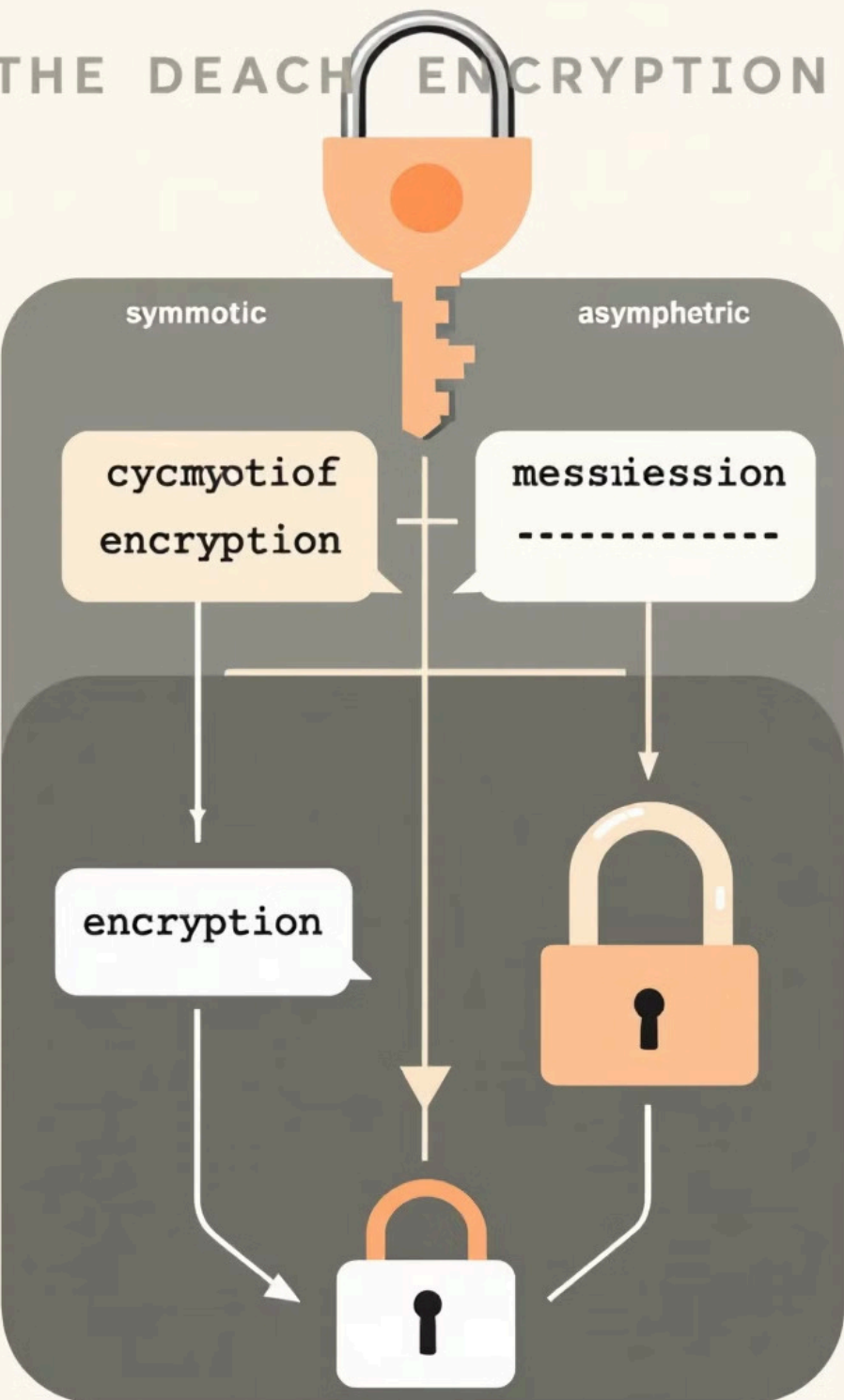
Mètode lleuger que no exigeix grans capacitats de xarxa. Ideal per a màquines distants o xarxes de capacitat escassa. Fàcil d'automatitzar mitjançant scripts.

Sessió amb interfície gràfica

Permet veure l'escriptori complet de l'estació remota. Requereix més capacitat de xarxa, generalment només disponible dins d'una LAN.

Client o eina d'administració local

Utilitza aplicacions locals o pàgines web per a l'administració. No exigeix gran capacitat de xarxa i ofereix una interfície més intuïtiva.



Introducció a la criptografia

Objectius de la criptografia

Assegurar la confidencialitat dels missatges, autenticar l'emissor i el destinatari, i garantir la integritat del missatge durant la transmissió.

Criptografia simètrica

Utilitza la mateixa clau per encriptar i desencriptar. Ràpida però requereix un canal segur per intercanviar la clau.

Criptografia asimètrica

Utilitza parelles de claus públiques i privades. Més segura per a l'intercanvi de claus però més lenta en l'encriptació/desencriptació.

Criptografia híbrida

Combina els avantatges de la simètrica i l'asimètrica, utilitzant clau pública per intercanviar una clau compartida i després encriptació convencional.

Secure Shell (SSH)

1

Què és SSH?

Protocol de xarxa que permet l'intercanvi d'informació de forma segura, utilitzant encriptació i criptografia de clau pública.

2

Funcionalitats

Iniciar sessions remotes, transmetre fitxers de manera segura, crear túnels per assegurar serveis no encriptats, i reenviament de sessions X11.

3

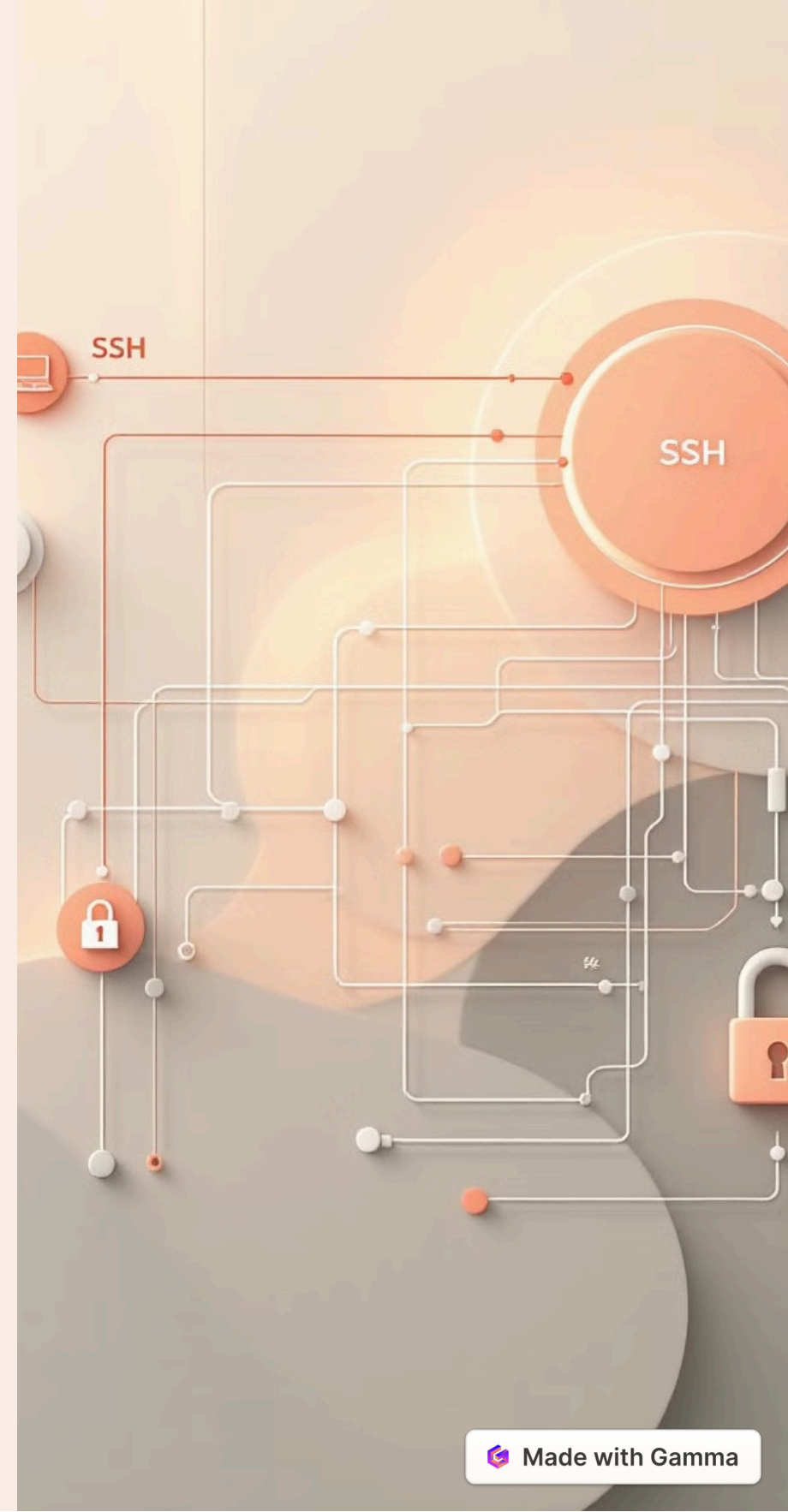
Procés de connexió

El client inicia la connexió, es negocia la versió del protocol i l'algoritme de xifrat, s'intercanvien claus públiques i es genera una clau de sessió.

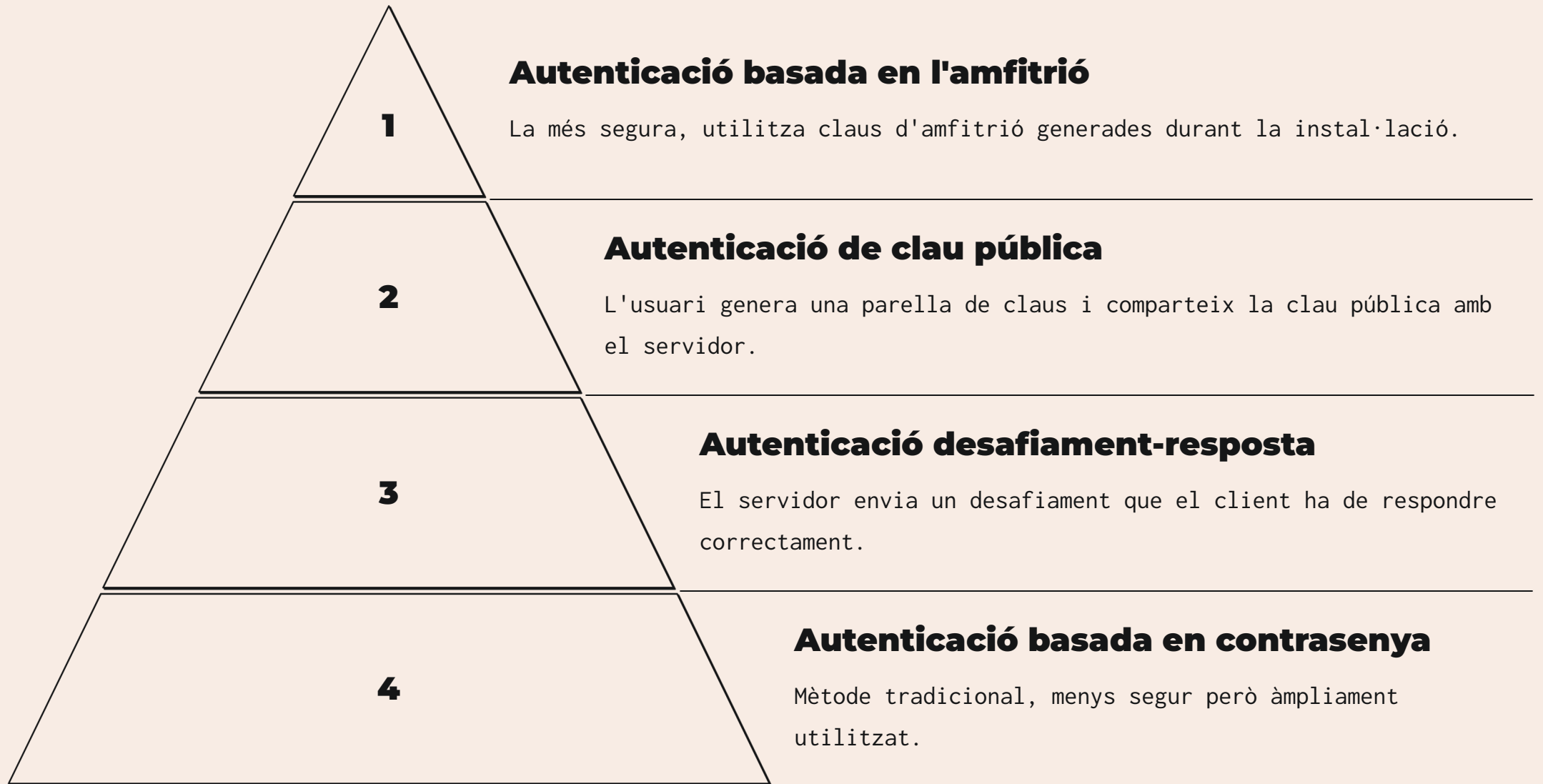
4

Autenticació

Pot utilitzar diversos mecanismes: basada en l'amfitrió, de clau pública, desafiament-resposta, o basada en contrasenya.



Autenticació en SSH



Tots aquests mètodes s'estableixen després d'una connexió encriptada inicial entre client i servidor.

Transferència segura d'arxius - scp

La comanda scp funciona de manera similar a cp per a còpies locals, però permet la transferència segura entre màquines remotes. Utilitza el protocol SSH per a la transferència.

1

Sintaxi bàsica

```
scp [opcions] [usuari@]host:fitxer_origen  
[usuari@]host:fitxer_destí
```

2

Còpia local a remot

```
scp fitxer_local.txt usuari@host_remot:/ruta/destí/
```

3

Còpia remot a local

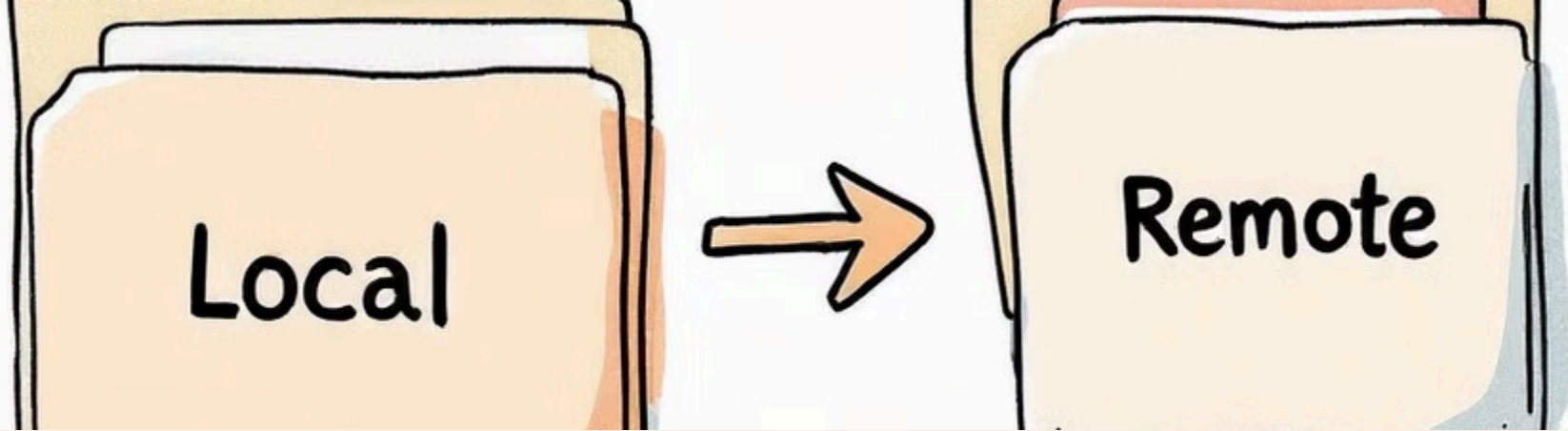
```
scp usuari@host_remot:/ruta/origen/fitxer_remot.txt  
/ruta/destí/
```

4

Còpia recursiva

```
scp -r directori_local/ usuari@host_remot:/ruta/destí/
```





Sincronització de directoris amb rsync

Rsync és una eina potent per sincronitzar fitxers i directoris entre diferents ubicacions, ja sigui en la mateixa màquina o entre màquines remotes.

1 Sintaxi bàsica

```
rsync [opcions] [origen] [destí]
```

2 Opcions comunes

-a (arxiu), -v (verbose), -z (compressió), -P (progrés), --delete (elimina fitxers no existents en l'origen)

3 Sincronització local

```
rsync -av /ruta/origen/ /ruta/desti/
```

4 Sincronització remota

```
rsync -av -e ssh /ruta/origen/  
usuari@host_remot:/ruta/desti/
```

Resum i consideracions finals

1

Seguretat

Utilitzeu sempre protocols segurs com SSH per a l'accés remot.

2

Autenticació

Preferiu l'autenticació de clau pública sobre les contrasenyes.

3

Sincronització

Rsync és una eina potent per mantenir directoris actualitzats.

4

Pràctica

Experimenteu amb diferents eines per trobar la millor per a cada tasca.

L'accés remot segur és essencial en l'era digital actual. Dominar aquestes eines i protocols us permetrà treballar de manera eficient i segura des de qualsevol lloc.