Accesso da postazione remota mediante protocollo ssh

- L'utente usa un terminale nella macchina client autenticandosi **mediante un account del client** (account_client).
- Nel server un processo sshd attende richieste di connessione.
- L'utente si connette con ssh alla macchina server e si autentica **sfruttando un account del server** (account_server).
- L'account del server in generale è diversa dall'account del client.
- **I comandi che l'utente digita nel terminale del client sono eseguiti sul server** da un interprete di comandi**.**
- **L'output dei comandi eseguiti sul server viene visualizzato nel terminale del client.**
- Tutti ciò che passa dalla connessione viene cifrato e quindi non è visibile a terzi

Autenticazione ssh mediante password

- L'utente si connette con ssh alla macchina server, specifica l'account sul server e, quando gli viene richiesto, fornisce la password dell'account_server.

  ssh account_server@nome_host_server

- Occorre quindi una azione non automatizzabile dell'utente, cioè digitare una password

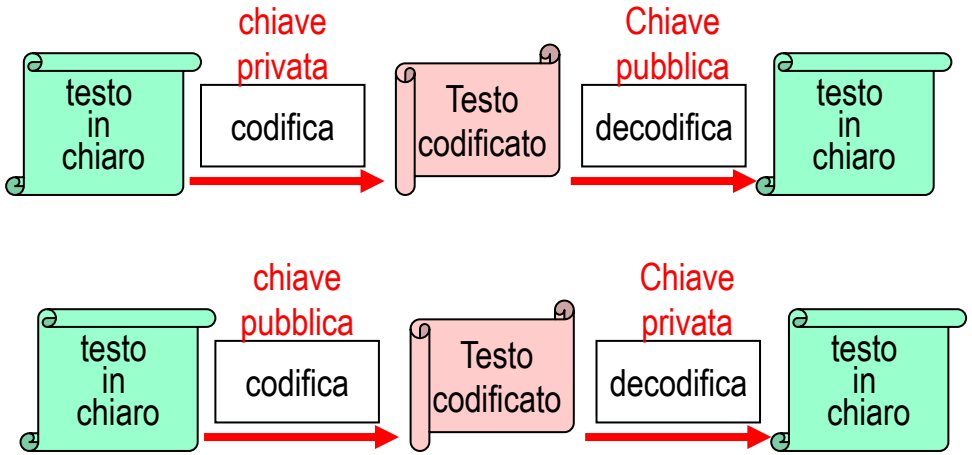
CRITTOGRAFIA A CHIAVE PUBBLICA (o asimmetrica)

Crittografia:

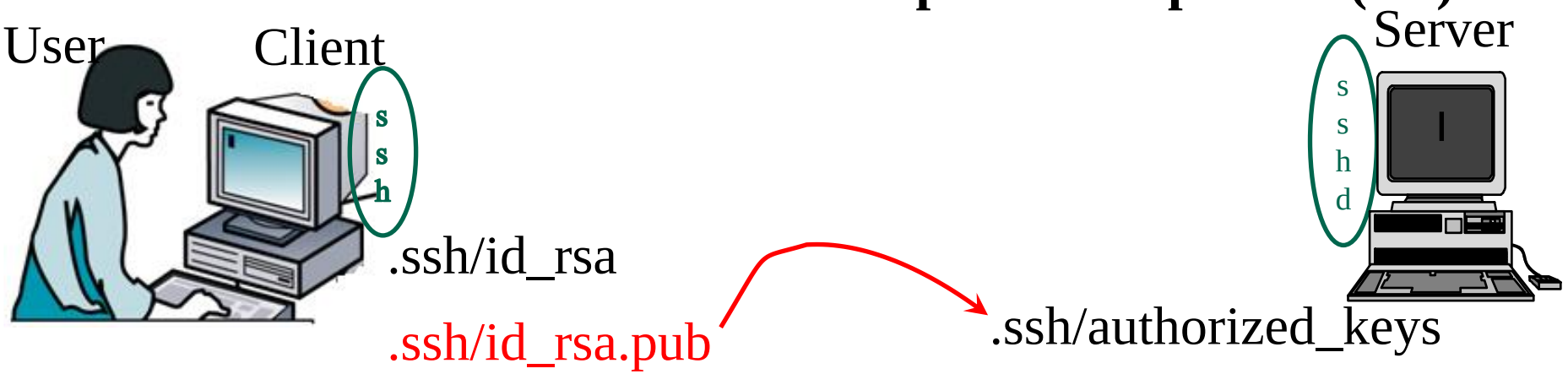
- Si codifica il testo (in chiaro) usando un algoritmo noto ed una prima chiave di cifratura ottenendo un testo incomprensibile (cifrato) che può essere trasmesso.
- Si decodifica il testo cifrato usando un algoritmo noto ed una seconda chiave di cifratura riottenendo il testo originale.

Crittografia a chiave pubblica:

- Algoritmo di codifica/decodifica RSA (*Rivest, Shamir e Adelson*)
- Si usano chiavi di 1024-2048 bit. Sotto 2048 bit sono meno sicure.
- Ogni utente ha una **coppia di chiavi** (una **privata** da mantenere segreta ed una **pubblica** da rendere nota a tutti).
- Entrambe le chiavi possono essere usate per codificare.
- Il testo codificato con una chiave può essere decodificato solo con l'altra chiave.



Autenticazione ssh mediante chiave pubblica e privata (1/3)



Operazioni preliminari sul client

• L'utente (account client) sul client crea una coppia di chiavi, pubblica e privata con il seguente comando:

ssh-keygen -t rsa

• Il comando colloca la chiave privata nella home directory dell'utente sul client, nel file .ssh/id_rsa La chiave privata deve rimanere segreta!

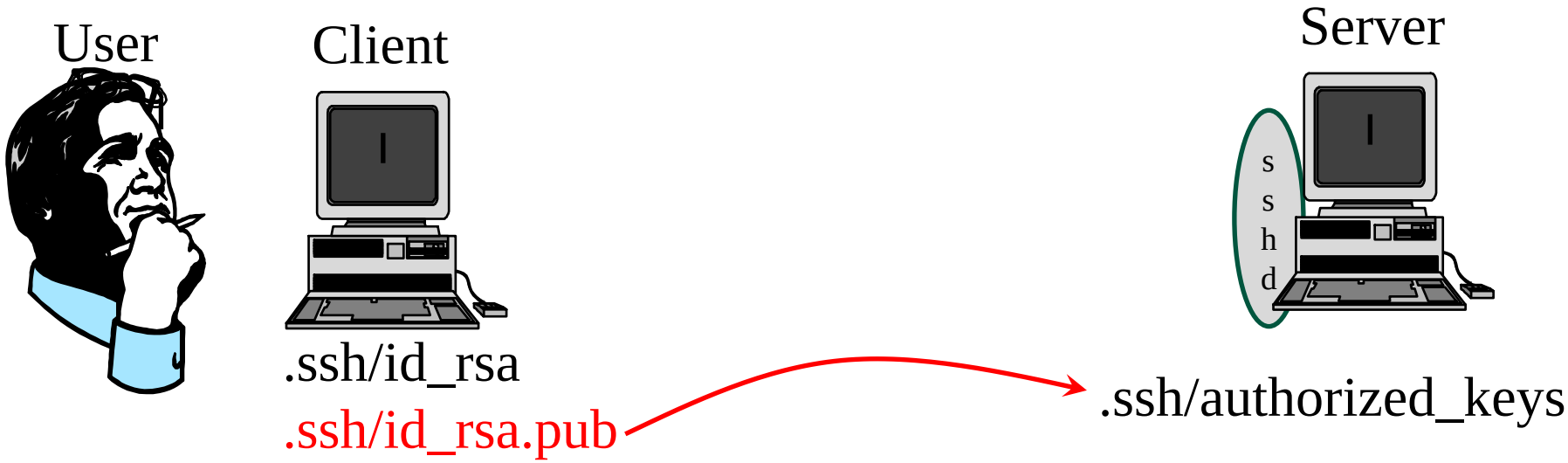
• La chiave pubblica viene invece collocata nel file .ssh/id_rsa.pub

Operazioni preliminari sul server

• La **chiave pubblica dell'account client deve essere copiata** nella home directory **dell'utente del server** (account server) nel file .ssh/authorized_keys

scp ~/.ssh/id_rsa.pub account_server@nome_host_server:.ssh/authorized_keys

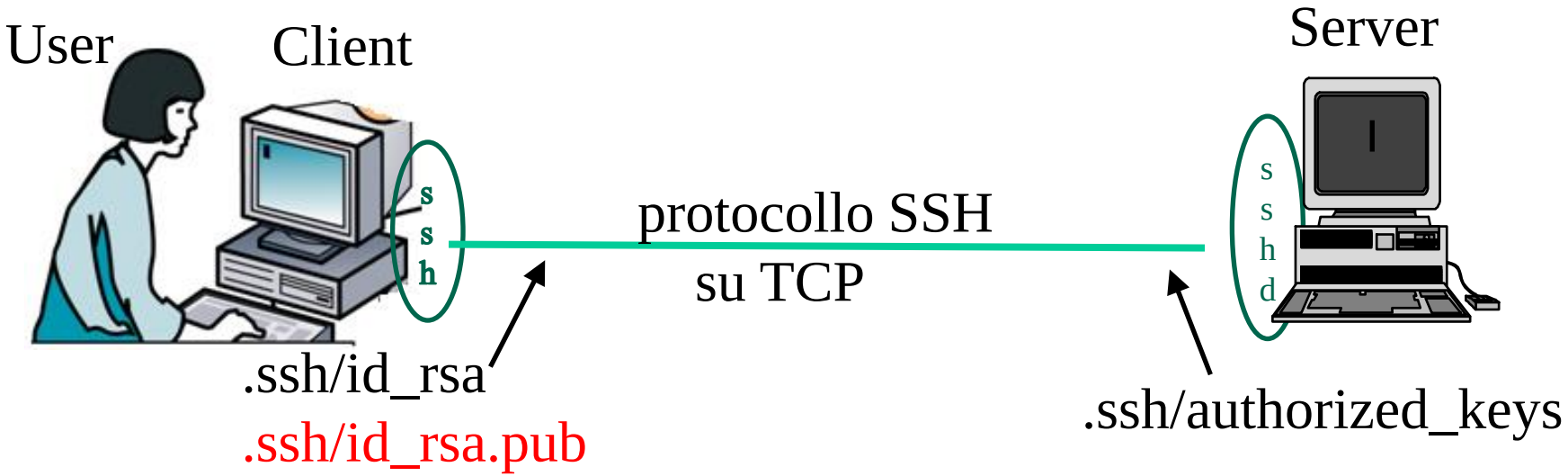
Autenticazione ssh mediante chiave pubblica e privata (2/3)



Esempio di chiave pubblica contenuta in .ssh/id_rsa.pub del client e poi copiata in .ssh/authorized_keys del server

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDVzguHcdZV8oWA1xfZMcS5sRsBLdjAKK
n0k2ZWaVe4Hi4gnDDzkkYlrK01lHwLcT+6xDGb7oqdErDVkdUm4/P7grkIXfh7
+2J1Dbd+xnGco2I71SwudiLCamvkufno0Pm9fooWm3q+EA1jpL4bH5ldqQBzMe
OuVAD2w/0Gqtuf9yR6fmpFFtgXePtQUOJqrV+KYeQcDX1p6dN6/eEOZRDaMq5i
UIex+ewilXet7uGhlK8C55/ONJfN3gRWOlzsIGn3baY6WTz41xL9F9al53RoPX
TKkRLD0RDdtkvRvG6hZDCEYYRj9uFRCoHtLChbtFwWRDWlIkvD/Rcf98Q0J23j
cW7ArRAZ08pRxCiyq45g30ZZHMt0VvrJfeQ5UO0nRktmFm1Rvfy3M1Bysq6hPB
XATtSp+4j4ckT4PgNx8qz6Itaz0Fx2fjHk+dFdRNhcEy2a9UGKZ3GS+6XDOyex
EyAlQphvl2HiqBc/3eXzljk8wXQLbZNFpheMayTU2zvaD2c=
account_client@nome_host_client
```

Autenticazione ssh mediante chiave pubblica e privata (3/3)



Connessione ssh a server remoto

• L'utente (account client) sul client esegue la connessione ssh con il seguente comando:

ssh account_server@nome_host_server

• I due end system sfruttano la coppia di chiavi per creare nuove chiavi e con queste cifrare le comunicazioni e renderle non leggibili dal terzi.

Se l'utente vuole comunque usare la passsword invece delle chiavi, può eseguire ssh aggiungendo altri parametri

ssh account_server@nome_host_server -o PubkeyAuthentication=no

Esecuzione comandi su server remoto mediante ssh

Lancio sequenza di comandi dal client ed esecuzione sul server remoto

```
ssh -T ghini@dancairo.cs.unibo.it /bin/bash <<FINESCRIPT
    echo inizio script
    pwd
    find ./ -name "prova.c"
    echo fine script
FINESCRIPT
```

Sequenza di comandi che la bash sul server legge ed esegue

Nell'esempio, "dancairo.cs.unibo.it" è il nome del server

"ghini" è l'account dell'utente nel server

"/bin/bash" è il comando da eseguire sul server

La stringa "FINESCRIPT" indica dove inizia e finisce la sequenza di comandi che la bash sul server legge "da tastiera" ed esegue.

Esecuzione script locali su server remoto mediante ssh

Script sul client da eseguire sul server remoto:

file script_da_eseguire_in_remoto.sh

```
echo inizio script
pwd
find ./ -name "prova.c"
echo fine script
```

Lancio di script dal client ed esecuzione sul server remoto

```
CODICE=`cat ./script_da_eseguire_in_remoto.sh`
ssh -T ghini@dancairo.cs.unibo.it /bin/bash <<FINESCRIPT
   echo ${CODICE}
FINESCRIPT
```