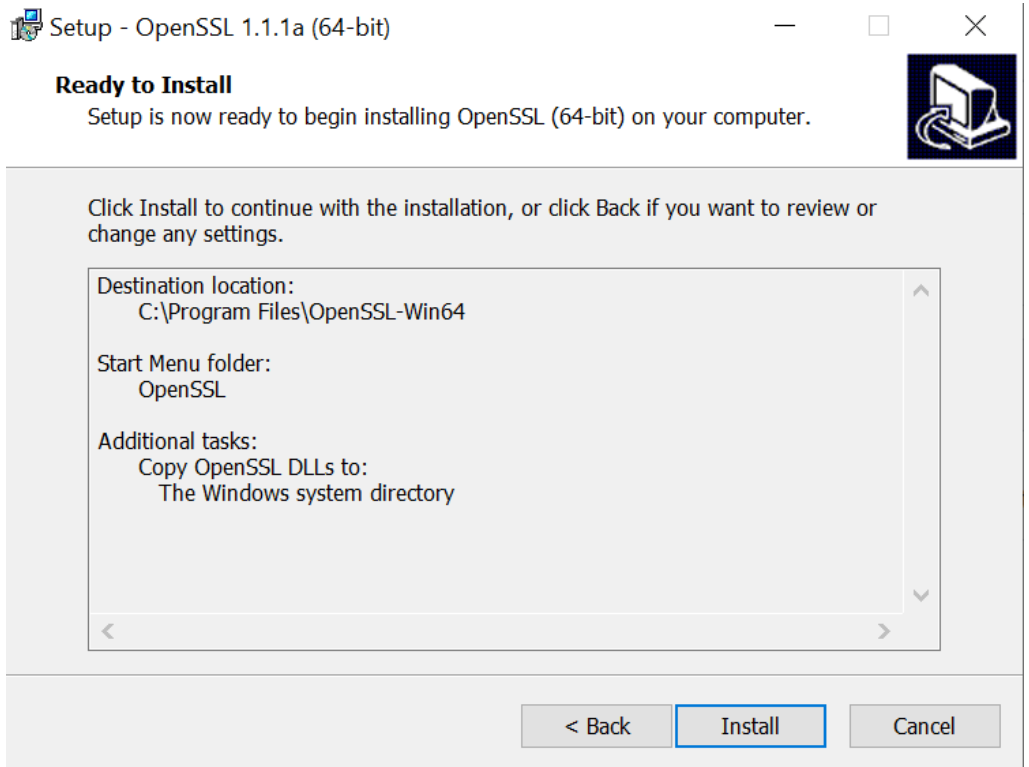
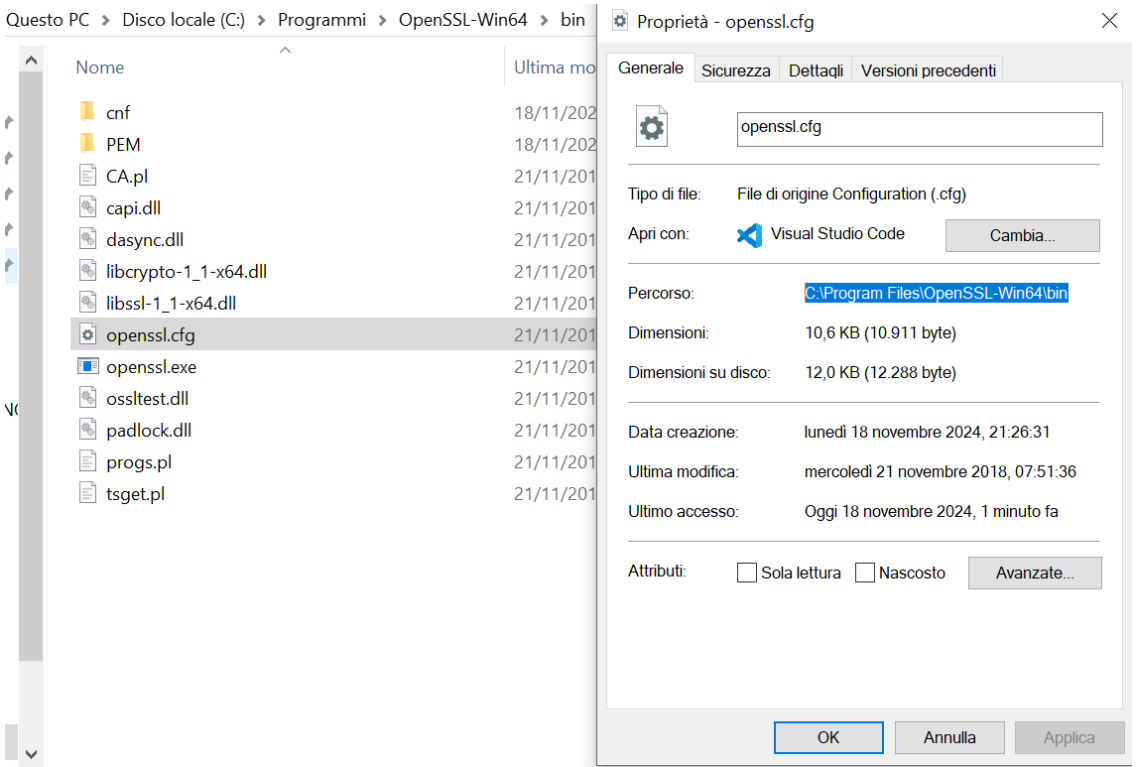
Encrypting e Decrypting di un messaggio con OpenSSL

Encrypting e Decrypting di un messaggio con OpenSSL

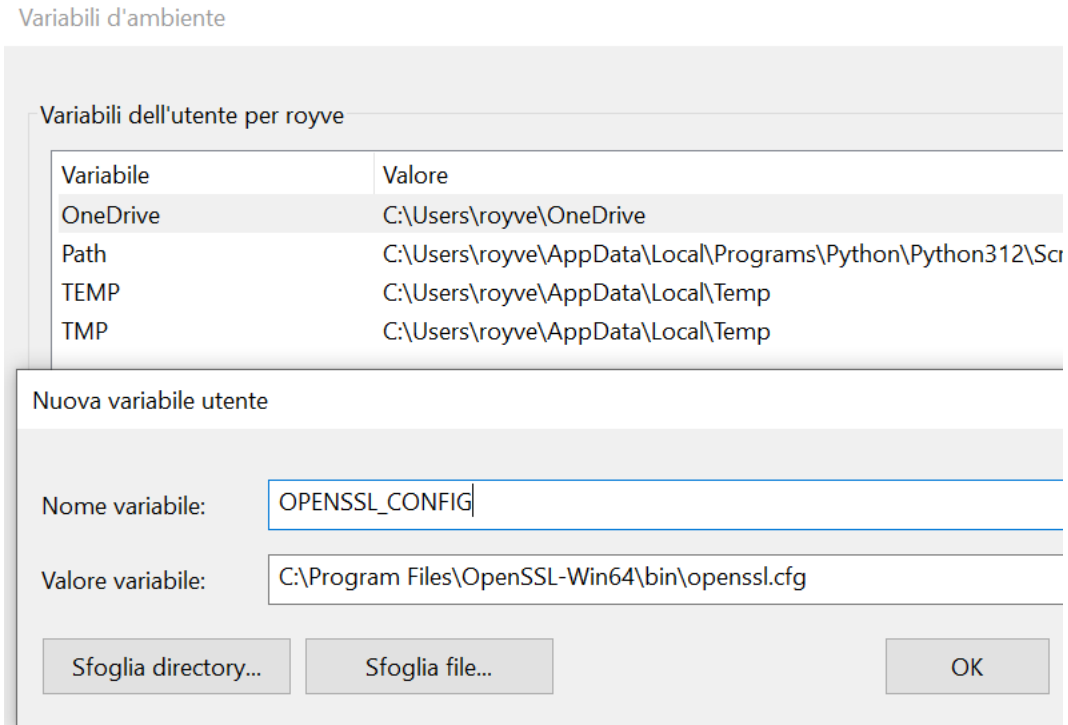
Una volta installato OpenSSL copio il path da inserire nelle variabili d'ambiente…

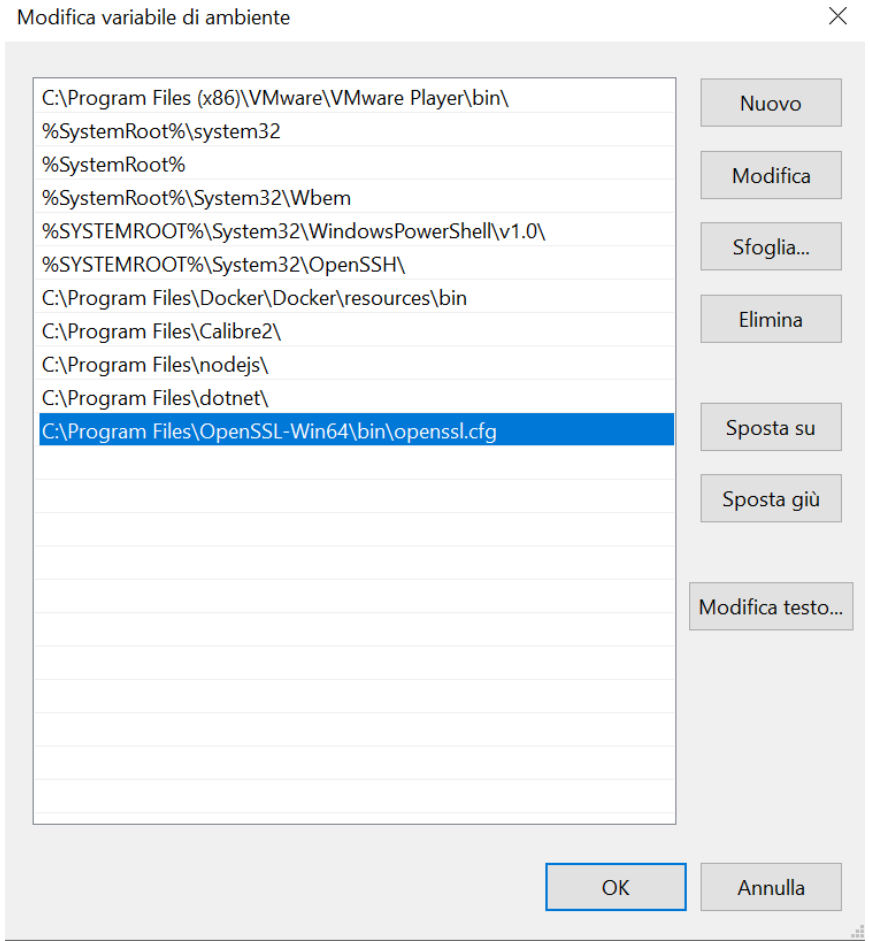




Encrypting e Decrypting di un messaggio con OpenSSL

...prima in quelle d'utente e poi in quelle di sistema.



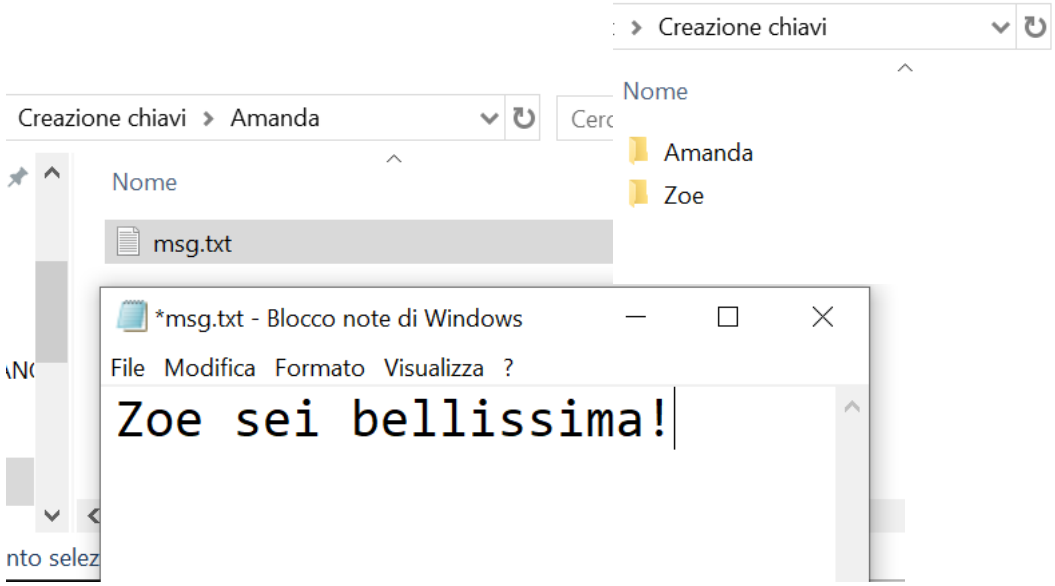


Encrypting e Decrypting di un messaggio con OpenSSL

Verifichiamo l'installazione e creiamo le 2 directory su cui lavoreremo, la cartella Amanda che è il mittente e Zoe è il destinatario, predisponiamo il messaggio che Amanda deve encrittare ed inviare a Zoe.

Prompt dei comandi

```
Microsoft Windows [Versione 10.0.19045.5131]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\royve>openssl
help:

Standard commands
asn1parse         ca                ciphers           cmp
cms               crl               crl2pkcs7         dgst
dhparam           dsa               dsaparam          ec
ecparam           enc               engine            errstr
fipsinstall       gendsa            genpkey           genrsa
help              info              kdf               list
mac               nseq              ocsp              passwd
pkcs12            pkcs7             pkcs8             pkey
pkeyparam         pkeyutl           prime             rand
rehash            req               rsa               rsautl
s_client          s_server          s_time            sess_id
smime             speed             spkac             srp
storeutl          ts                verify            version
x509
```



Encrypting e Decrypting di un messaggio con OpenSSL

Apriamo due prompt di comandi per le 2 cartelle, generiamo entrambe le chiavi nelle rispettive directory.

```
C:\Users\royve\Desktop\betalent\Creazione chiavi\Amanda>openssl genrsa -out am
anda.key 4096

C:\Users\royve\Desktop\betalent\Creazione chiavi\Amanda>dir
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 0065-921C

 Directory di C:\Users\royve\Desktop\betalent\Creazione chiavi\Amanda

18/11/2024  22:41    <DIR>          .
18/11/2024  22:41    <DIR>          ..
18/11/2024  22:41             3.324 amanda.key
18/11/2024  22:16                 0 msg.txt
               2 File          3.324 byte
               2 Directory  603.454.177.280 byte disponibili
```

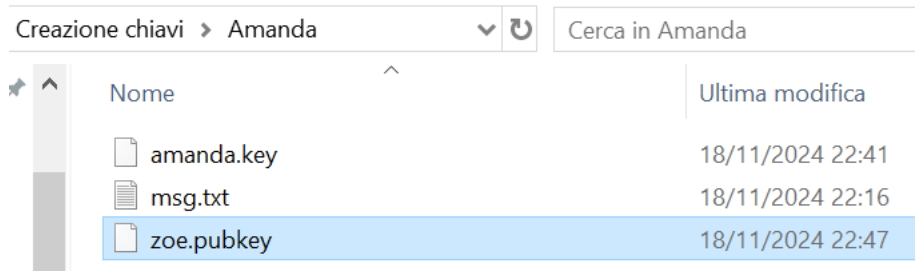
```
C:\Users\royve\Desktop\betalent\Creazione chiavi\Zoe>openssl genrsa -out zoe.key 40
96

C:\Users\royve\Desktop\betalent\Creazione chiavi\Zoe>dir
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 0065-921C

 Directory di C:\Users\royve\Desktop\betalent\Creazione chiavi\Zoe

18/11/2024  22:42    <DIR>          .
18/11/2024  22:42    <DIR>          ..
18/11/2024  22:42             3.324 zoe.key
               1 File          3.324 byte
               2 Directory  603.454.554.112 byte disponibili
```

Encrypting e Decrypting di un messaggio con OpenSSL

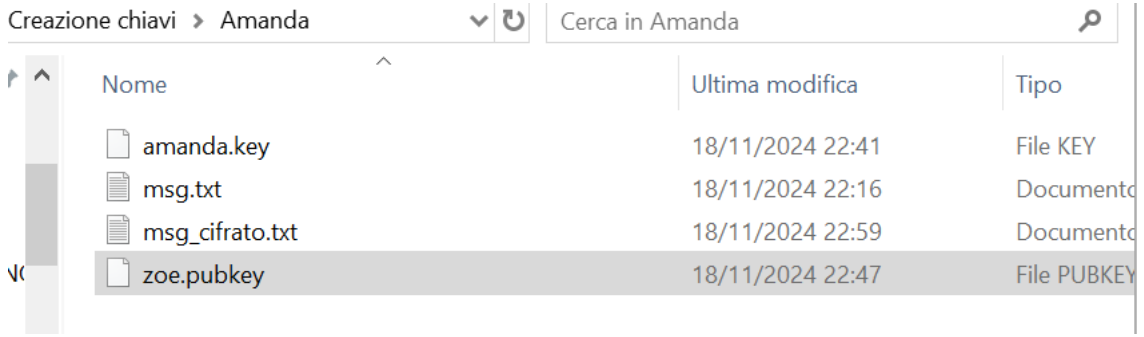
Dalle chiavi generate per Zoe (destinatario) estraiamo la chiave pubblica(pubkey) e la copiamo nella cartella di Amanda (mittente), in modo che Amanda la potrà usare per cifrare il messaggio.

Procediamo con la cifratura del messaggio dalla cartella di Amanda usando la pubkey di Zoe. **Pkeyutl** è la utility che usiamo per l'encrypt e il decrypt, **rsa e pubout** sono state utilizzate invece per ottenere la chiave pubblica dalla coppia di chiavi.

```
C:\Users\royve\Desktop\betalent\Creazione chiavi\Zoe>openssl rsa -in zoe.key -pubou
t -out zoe.pubkey
writing RSA key
```




```
C:\Users\royve\Desktop\betalent\Creazione chiavi\Amanda>openssl pkeyutl -encry
pt -in msg.txt -pubin -inkey zoe.pubkey -out msg_cifrato.txt
```



Encrypting e Decrypting di un messaggio con OpenSSL

Copio il messaggio cifrato nella cartella di Zoe che procede col decrypting usando la sua chiave privata.