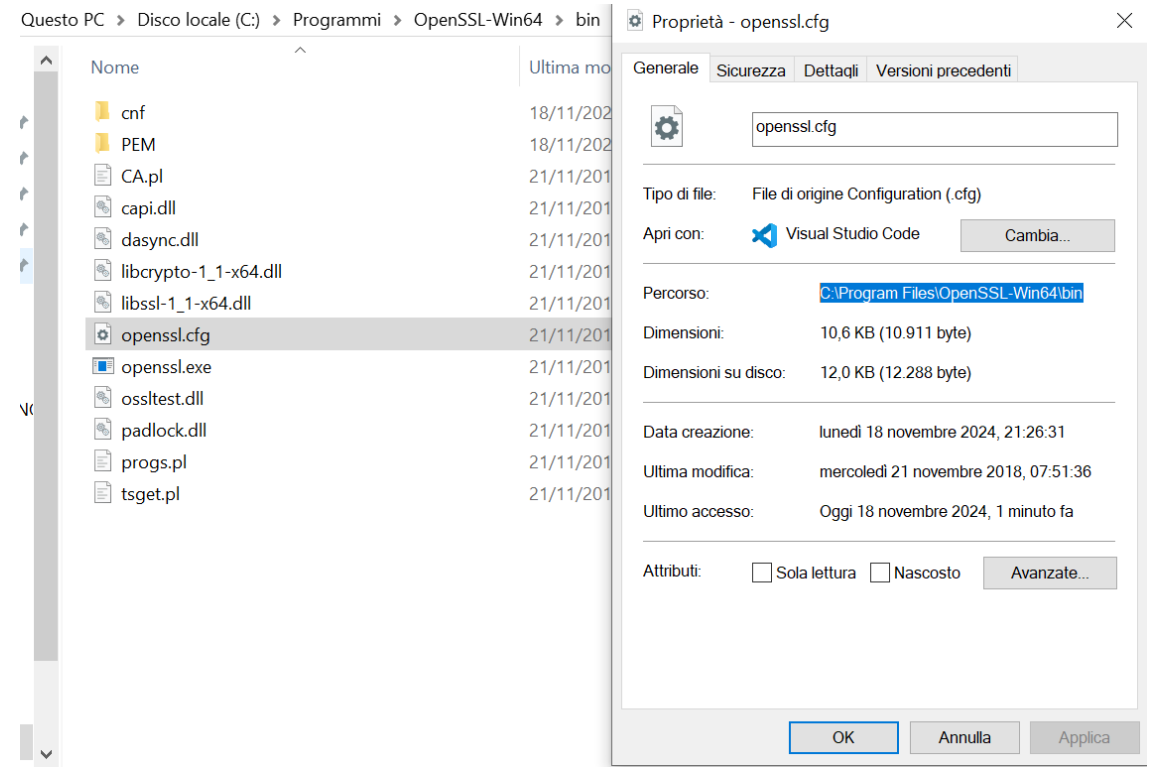
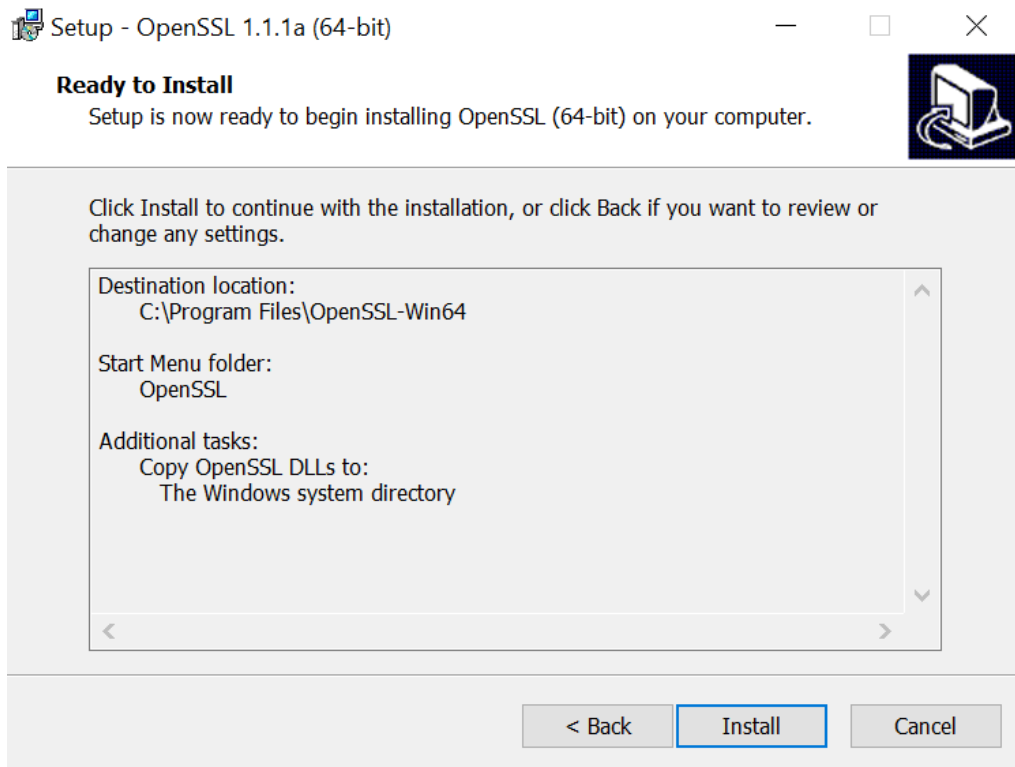




Encrypting e Decrypting di un messaggio con OpenSSL

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.

Variabili d'ambiente

Variabili dell'utente per royve

Variabile	Valore
OneDrive	C:\Users\royve\OneDrive
Path	C:\Users\royve\AppData\Local\Programs\Python\Python312\Scr
TEMP	C:\Users\royve\AppData\Local\Temp
TMP	C:\Users\royve\AppData\Local\Temp

Nuova variabile utente

Nome variabile:

OPENSSL_CONFIG

Valore variabile:

C:\Program Files\OpenSSL-Win64\bin\openssl.cfg

Sfoggia directory...

Sfoggia file...

OK

Modifica variabile di ambiente

C:\Program Files (x86)\VMware\VMware Player\bin\
%SystemRoot%\system32
%SystemRoot%
%SystemRoot%\System32\Wbem
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
%SYSTEMROOT%\System32\OpenSSH\
C:\Program Files\Docker\Docker\resources\bin
C:\Program Files\Calibre2\
C:\Program Files\nodejs\
C:\Program Files\dotnet\
C:\Program Files\OpenSSL-Win64\bin\openssl.cfg

Nuovo

Modifica

Sfoggia...

Elimina

Sposta su

Sposta giù

Modifica testo...

OK

Annulla

Encrypting e Decrypting di un messaggio con OpenSSL

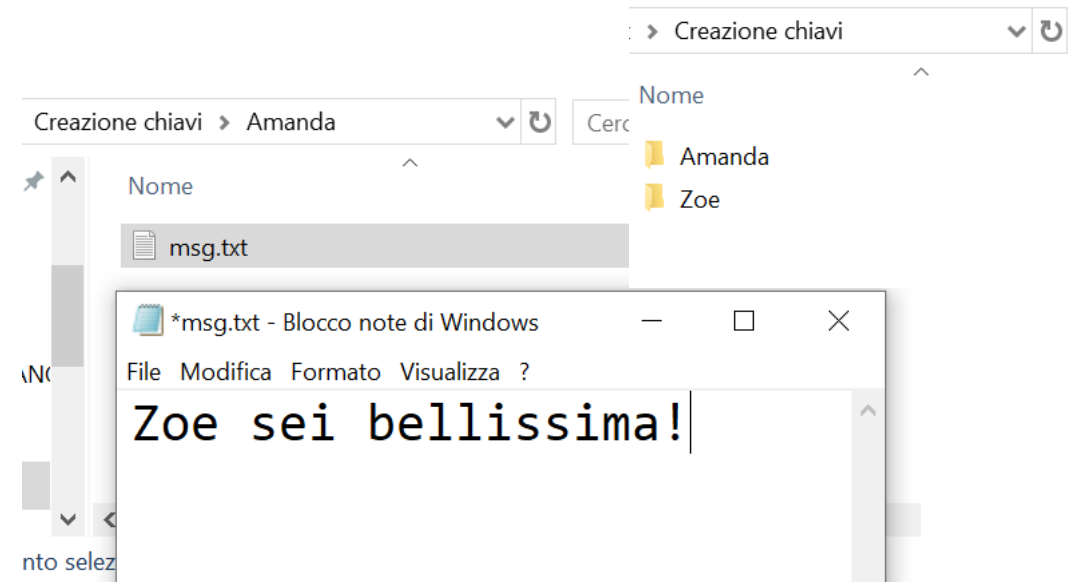
Verifichiamo l'installazione e creiamo le 2 directory su cui lavoreremo, la cartella Amanda che è il mittente e Zoe è il destinatario, predisponiamo il messaggio che Amanda deve encrittare ed inviare a Zoe.

```
C:\> 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        ocsf              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 amanda.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 4096

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.
Pkeyutil 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 -pubout -out zoe.pubkey  
writing RSA key
```

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

Creazione chiavi > Amanda		Cerca in Amanda
Nome	Ultima modifica	
amanda.key	18/11/2024 22:41	
msg.txt	18/11/2024 22:16	
zoe.pubkey	18/11/2024 22:47	

Creazione chiavi > Amanda		Cerca in Amanda
Nome	Ultima modifica	Tipo
amanda.key	18/11/2024 22:41	File KEY
msg.txt	18/11/2024 22:16	Document
msg_cifrato.txt	18/11/2024 22:59	Document
zoe.pubkey	18/11/2024 22:47	File PUBKEY

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.

