Cifratura Simmetrica con OpenSSL

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

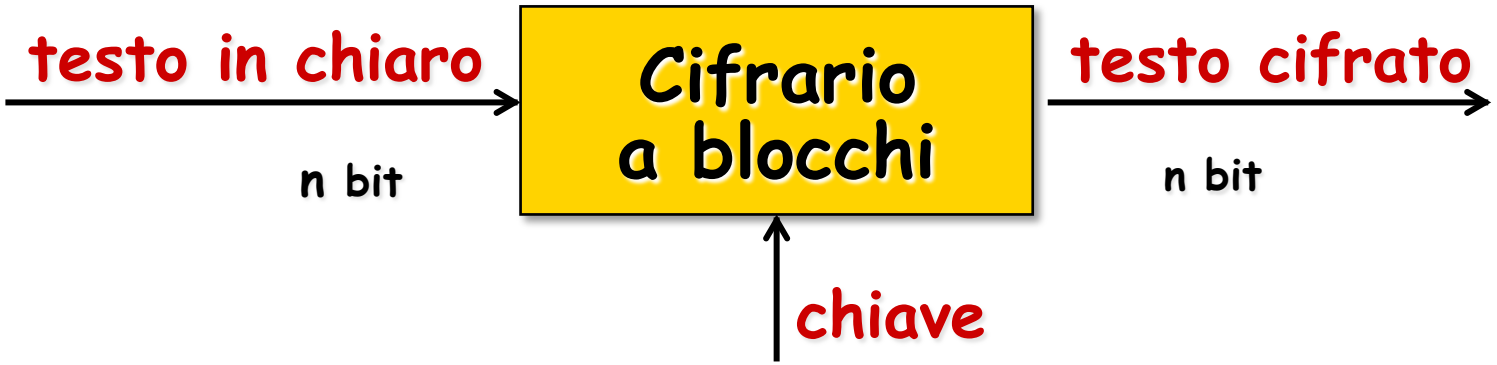
http://www.dia.unisa.it/professori/ads

Marzo 2017

Cifrari simmetrici

- Crittosistemi a chiave privata/segreta
- Alice e Bob conoscono la stessa chiave K
- Cifrari a blocchi
  - Messaggi divisi in blocchi e poi cifrati
- Stream cipher
  - Messaggi cifrati carattere per carattere

Cifrari a blocchi



- Alcuni esempi:
  - Data Encryption Standard (DES)
  - DES triplo
  - Blowfish
  - Advanced Encryption Standard (AES)

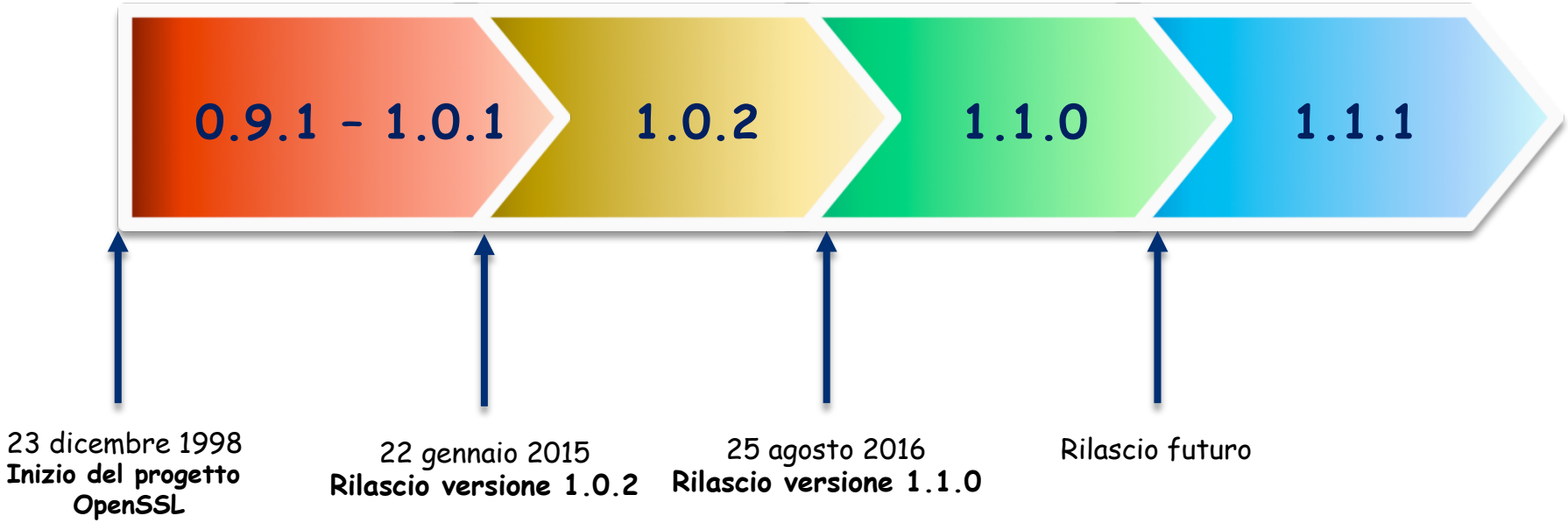
OpenSSL

- Progetto Open Source nato nel dicembre del 1998
- OpenSSL fornisce implementazioni per
  - Funzioni Crittografiche
  - Protocolli quali Secure Sockets Layer (SSL) e Transport Layer Security (TLS)
- OpenSSL comprende
  - Comandi eseguibili per funzioni crittografiche
  - Libreria contenente API per sviluppare applicazioni crittografiche
- OpenSSL supporta crittografia basata su curve ellittiche
  - Elliptic Curve Cryptography (ECC)

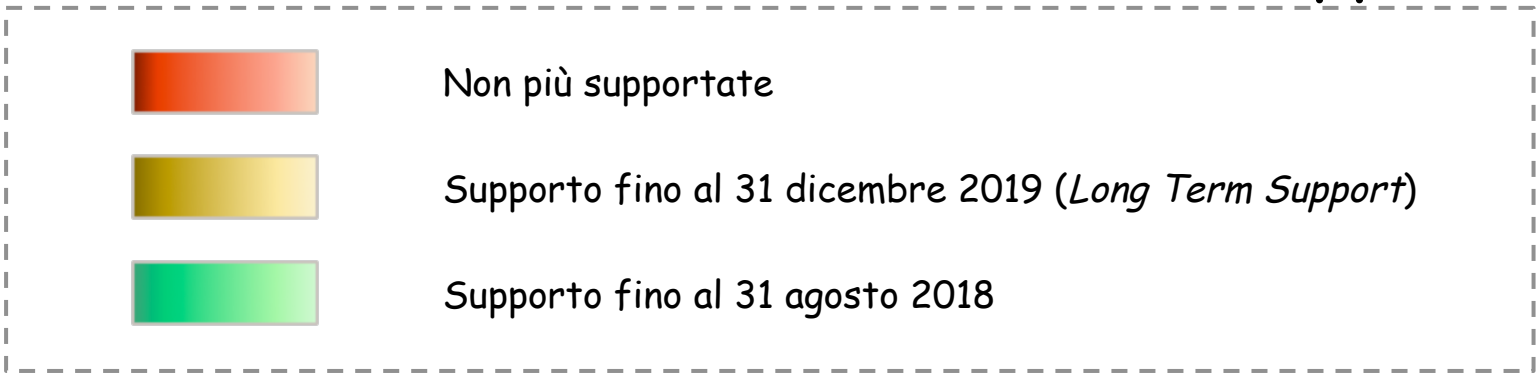
"The Swiss Army knife of cryptography"

OpenSSL™
Cryptography and SSL/TLS Toolkit

OpenSSL Versioning



Supporto



OpenSSL Versioning

- A partire dalla versione 1.0.0, OpenSSL ha adottato un particolare schema di versioning
  - *Letter releases:* Contengono esclusivamente correzioni riguardanti bug e sicurezza, ma non nuove funzionalità
    - 1.0.2**a**, 1.0.2**b**
  - *Releases that change the last digit:* Possono contenere (e di solito contengono) nuove funzionalità, pur rimanendo retrocompatibili con la versione precedente
    - 1.0.**1** vs. 1.0.**2**
    - 1.1.**0** vs 1.1.**1**

https://www.openssl.org/policies/releasestrat.html
https://www.openssl.org/news/changelog.html

Ambiente di Lavoro Consigliato

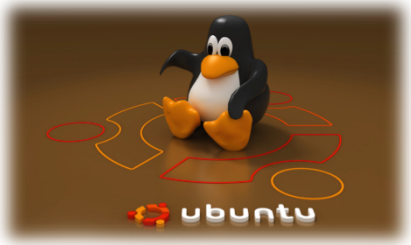
- Per esercitarsi con OpenSSL è fortemente consigliato l'utilizzo di
  - OpenSSL in versione maggiore o uguale di 1.0.2
    - Versioni ancora supportate
  - Sistema Operativo Linux
    - Per maggiori dettagli riguardanti le varie distribuzioni
      - https://distrowatch.com/
    - **N.B. A prescindere dalla distribuzione utilizzata, è bene usare sempre la relativa ultima versione**

DistroWatch.com
Put the fun back into computing. Use Linux, BSD.

OpenSSL
Cryptography and SSL/TLS Toolkit

Ambiente di Lavoro Utilizzato per gli Esempi

- Gli esempi mostrati in classe sono stati sviluppati utilizzando il seguente ambiente software
  - Linux Ubuntu 16.04 LTS (long-term support)
  - OpenSSL versione 1.0.2.g
- È possibile installare Linux
  - Nativamente su una macchina
  - In macchina virtuale (ad es. usando VirtualBox)
  - Direttamente in Windows 10 (Windows 10 Bash Shell)
    - https://www.howtogeek.com/249966/how-to-install-and-use-the-linux-bash-shell-on-windows-10/



Help

- Documentazione
  - https://www.openssl.org/docs/
- Manpage
  - https://www.openssl.org/docs/manmaster/man1/
- Cookbook (free download)
  - https://www.feistyduck.com/books/openssl-cookbook/
- Mailing list
  - https://www.openssl.org/community/mailinglists.html

OpenSSL™
Cryptography and SSL/TLS Toolkit

OpenSSL Wiki
(https://wiki.openssl.org/index.php/Main_Page)

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn among multiple locations and formats.

Contents [hide]

OpenSSL Quick Links [edit]

OpenSSL Overview	Compilation and Installation	Internals	Mailing Lists
libcrypto API	libssl API	Examples	Index of all API functions
License	Command Line Utilities	Related Links	Binaries
SSL and TLS Protocols	1.1 API Changes	FIPS modules	

OpenSSL Wiki

(https://wiki.openssl.org/index.php/Main_Page)

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn among multiple locations and formats.

Contents [hide]

OpenSSL Quick Links [ed

Panoramica generale su OpenSSL

OpenSSL Overview
libcrypto API
libssl API
Examples
Mailing Lists
Index of all API functions
License
Command Line Utilities
Related Links
Binaries
SSL and TLS Protocols
1.1 API Changes
FIPS modules

OpenSSL Wiki

(https://wiki.openssl.org/index.php/Main_Page)

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn among multiple locations and formats.

Contents [hide]

OpenSSL Quick Links [edit]

OpenSSL Overview
libcrypto API
License
SSL and TLS Protocols

Mailing Lists
Index of all API functions
Binaries

Informazioni sul protocollo SSL/TLS implementato da OpenSSL

OpenSSL Wiki

(https://wiki.openssl.org/index.php/Main_Page)

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn among multiple locations and formats.

Contents [hide]

OpenSSL Quick Links [edit]

OpenSSL Overview	Compilation and Installation	
libcrypto API	libssl API	
License	Command Line Utilities	
SSL and TLS Protocols	1.1 API Changes	FIPS modules

Funzionalità offerte da OpenSSL mediante linea di comando

OpenSSL Wiki
(https://wiki.openssl.org/index.php/Main_Page)

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn among multiple locations and formats.

Contents [hide]

OpenSSL Quick Links [edit]

OpenSSL Overview	Compilation and Installation	Internals	Ma
libcrypto API	libssl API	Examples	In
License	Command Line Utilities	Related Links	Bi
SSL and TLS Protocols	1.1 API Changes	FIPS modules	

Compatibilità di OpenSSL con lo standard **Federal Information Processing Standard (FIPS) 140-2** pubblicato dal NIST

http://csrc.nist.gov/groups/STM/cmvp/standards.html

Overview di OpenSSL

- OpenSSL fornisce
  - Un ampio insieme di comandi
  - Un ancora più ampio insieme di opzioni
    - Usate per raffinare e controllare ulteriormente i comandi

OpenSSL™
Cryptography and SSL/TLS Toolkit

Comandi OpenSSL
(Modalità Operative)

- Mediante il comando **openssl** possono essere richiamate da command-line tutte le funzionalità offerte da OpenSSL
- Il comando **openssl** può essere utilizzato in due *modalità operative*
  - **Interattiva:** Il comando **openssl** è invocato senza alcun parametro
    - Viene mostrato un prompt (>) dove digitare i comandi
    - Quando termina l'esecuzione di un comando, il prompt è mostrato di nuovo ed è pronto a processare un nuovo comando
    - Si può uscire da OpenSSL mediante il comando **quit**

```
$ openssl
OpenSSL>
```

  - **Batch:** Ciascun comando deve essere preceduto da "**openssl**"

```
$ openssl version
OpenSSL 1.0.2g 1 Mar 2016
```

Comandi OpenSSL
(Sintassi)

- La prima parte di un comando OpenSSL è data dal nome del comando stesso, seguito da tutte le opzioni che si intendono specificare, ciascuna separata da uno spazio
  - Le opzioni di solito iniziano con un trattino e spesso richiedono uno specifico parametro posto dopo uno spazio
- In generale, l'ordine in cui si specificano le opzioni non è significativo
  - Pochi casi in cui l'ordine è significativo
    - Di solito perché una specifica opzione deve apparire sulla command-line come ultima opzione specificata

Cifratura Simmetrica in OpenSSL

- OpenSSL fornisce numerosi cifrari simmetrici
  - La maggior parte di essi supporta varie modalità operative, ad es., ECB, CBC, CFB ed OFB
    - Per ciascun cifrario, la modalità operativa di default è CBC, se nessun'altra modalità è esplicitamente specificata
  - Si ricorda che la modalità ECB ha problemi di sicurezza, e si deve valutare se utilizzarla

Cifratura Simmetrica in OpenSSL

- Di solito i dati sono letti dallo standard input e scritti sullo standard output
  - Possono anche essere specificati file di input ed output
- Solo un singolo file alla volta può essere cifrato o decifrato
- Ciascun cifrario richiede una chiave per effettuare la cifratura o la decifratura
  - La chiave usata per cifrare i dati deve essere nota solo al mittente ed ai destinatari dei dati cifrati

Cifratura Simmetrica in OpenSSL

(Il Comando enc)

- Il comando **enc** (encrypt/encode) permette di accedere ai cifrari simmetrici forniti da OpenSSL

```
openssl enc args
```

- Ciascun cifrario può essere anche acceduto tramite un comando il cui nome inizia con quello del cifrario stesso

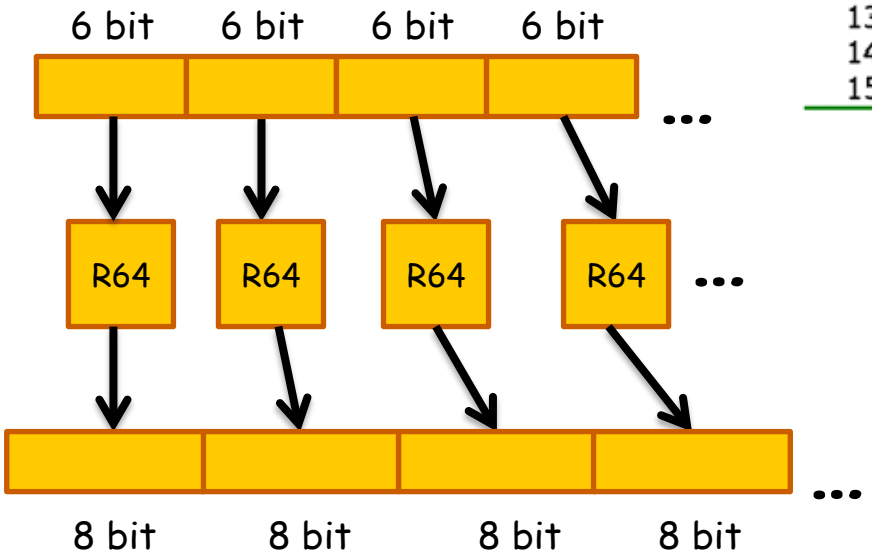
```
$ openssl
OpenSSL> des -in Originale.txt -out Cifrato
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
OpenSSL>
```

Codifica Base64

Base64
Set di caratteri formato
ASCII RADIX-64

valore	codifica	valore	codifica	valore	codifica	valore	codifica
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Tabella di conversione Base64



Dato un input di n byte, l'output della codifica avrà lunghezza pari a $4\lceil n/3 \rceil$

Espansione del 33%

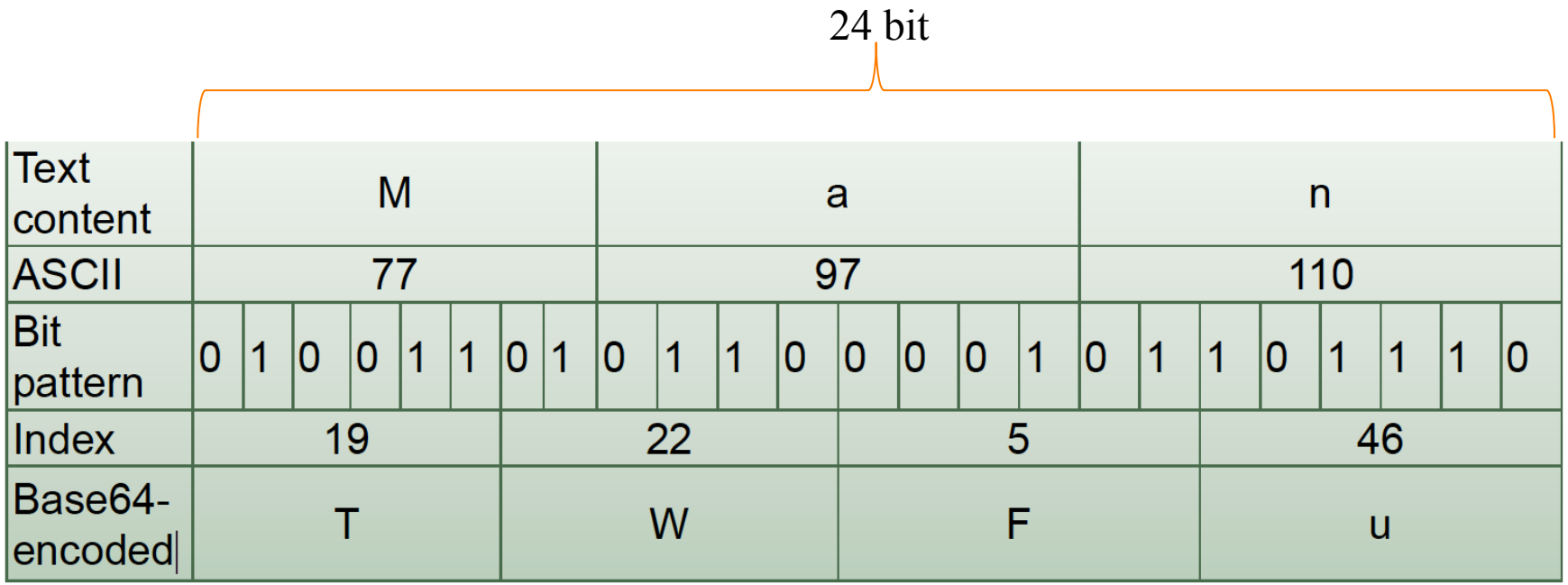
Codifica Base64

Il file in input è processato a blocchi da 24 bit

- Ciascun blocco è suddiviso in gruppi di 6 bit (a partire da sinistra)
- Viene considerato il valore decimale di ciascun gruppo di bit, tale valore rappresenterà un indice nella tabella di codifica Base64 (valori da 0 a 63)
  - Ogni indice viene convertito in caratteri ASCII, secondo la tabella di conversione Base64
  - Se il numero totale di bit da processare non è un multiplo di 24 viene utilizzato il padding
    - Vengono inseriti bit nulli (0) alla fine
    - Nella codifica viene inserito il simbolo '=' per ogni gruppo di 6 bit che manca per creare un blocco da 24 bit
      - Questo garantisce che l'output codificato in Base64 sia multiplo di 4 byte

Codifica Base64

(Esempio 1)



Per effettuare qualche prova
https://www.base64encode.org/

Codifica Base64

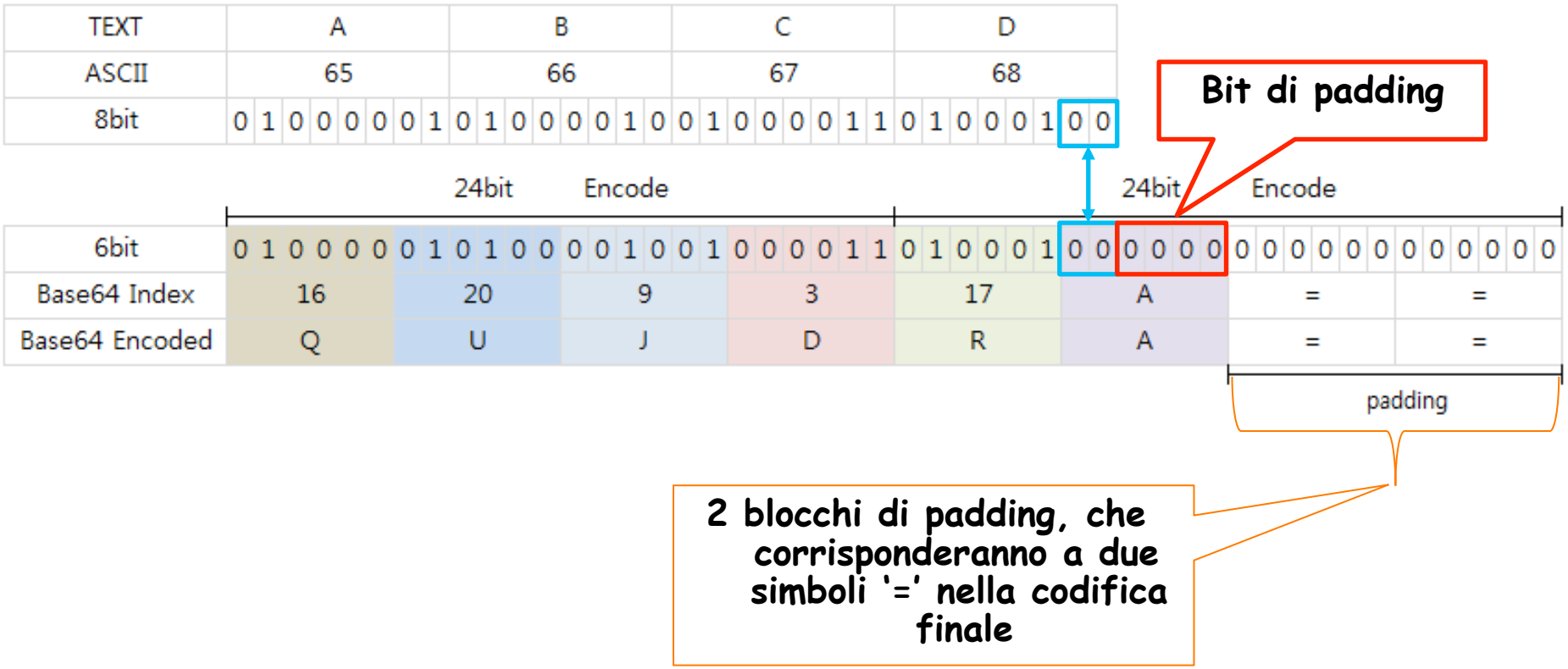
(Esempio 2)

TEXT	A	B	C	D
ASCII	65	66	67	68
8bit	0 1 0 0 0 0 0 1	0 1 0 0 0 0 1 0	0 1 0 0 0 0 1 1	0 1 0 0 0 1 0 0

	24bit Encode				24bit Encode			
6bit	0 1 0 0 0 0	0 1 0 1 0 0	0 0 1 0 0 1	0 0 0 0 1 1	0 1 0 0 0 1	0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Base64 Index	16	20	9	3	17	A	=	=
Base64 Encoded	Q	U	J	D	R	A	=	=
							padding	

Codifica Base64

(Esempio 2)



Codifica Base64 in OpenSSL

Per codificare un file in Base64 può essere usato il seguente comando

```
openssl enc -base64 -in input-file -out output-file
```

Per decodificare un file codificato in Base64 può essere usato il seguente comando

```
openssl enc -base64 -d -in input-file -out output-file
```

Cifratura Simmetrica in OpenSSL

Opzioni principali del comando enc

`openssl enc args`

- args
  - -ciphername
    - Tipo di cifrario, lunghezza della chiave e modalità operativa
    - Usare il comando `openssl list-cipher-commands` per ottenere la lista completa
  - -in filename
    - File di input
  - -out filename
    - File di output
  - -e or –d
    - Specifica se si tratta di cifratura o decifratura
  - -K key
    - Chiave usata dal cifrario per cifrare o decifrare. Se non viene specificata, OpenSSL deriverà questa chiave da una password
  - -pass arg
    - Sorgente della password. I valori possibili per `arg` sono `pass:password` o `pass:filename`, dove password è la `password` e `filename` è il file contenente la password. Se non si usa questo parametro viene mostrato un prompt per inserire la password
  - -base64
    - Applica la codifica base64 prima o dopo le operazioni crittografiche

Cifratura Simmetrica in OpenSSL

Opzioni principali del comando enc

`openssl enc args`

- **args**
  - **-ciphername**
    - **Tipo di cifrario e**
    - **Usare il comando** **ottenere la lista completa**
  - **-in filename**
    - **File di input**
  - **-out filename**
    - **File di output**
  - **-e or -d**
    - **Specifica se si tratta di cifratura o decifratura**
  - **-K key**
    - **Chiave usata dal cifrario per cifrare o decifrare. Se non viene specificata, OpenSSL deriverà questa chiave da una password**
  - **-pass arg**
    - **Sorgente della password. I valori possibili per `arg` sono `pass:password` o `pass:filename`, dove password è la `password` e `filename` è il file contenente la password. Se non si usa questo parametro viene mostrato un prompt per inserire la password**
  - **-base64**
    - **Applica la codifica base64 prima o dopo le operazioni crittografiche**

Per ottenere la lista completa delle opzioni del comando **enc** è possibile utilizzare **man enc**

Cifratura Simmetrica in OpenSSL

(Struttura di un Ciphername)

- Un ciphername è tipicamente composto da 3 parti, separate da un trattino '–' (è obbligatorio solo il nome del cifrario)
  - Nome del Cifrario
  - Lunghezza della Chiave (in bit)
  - Modalità Operativa

`cifrario-lunghezzaChiave-modalitaOperativa`

Esempio

`aes-256-cbc`

Cifratura Simmetrica in OpenSSL

(Cifratura)

Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura ché la diritta via era smarrita. Ahi quanto a dir qual era è cosa dura esta selva selvaggia e aspra e forte che nel pensier rinova la paura! Tant'è amara che poco è più morte; ma per trattar del ben ch'i' vi trovai, dirò de l'altre cose ch'i' v'ho scorte.

FileInChiaro.rtf

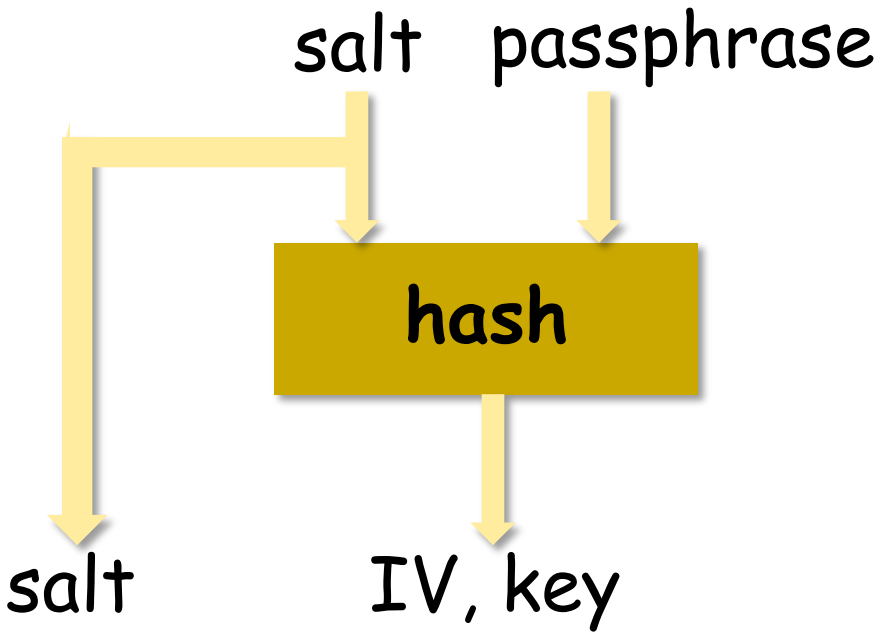
Cifratura

```
openssl enc -aes-256-cbc -in FileInChiaro.rtf -out FileCifrato.rtf -e -pass
pass:P1pp0B4ud0
```

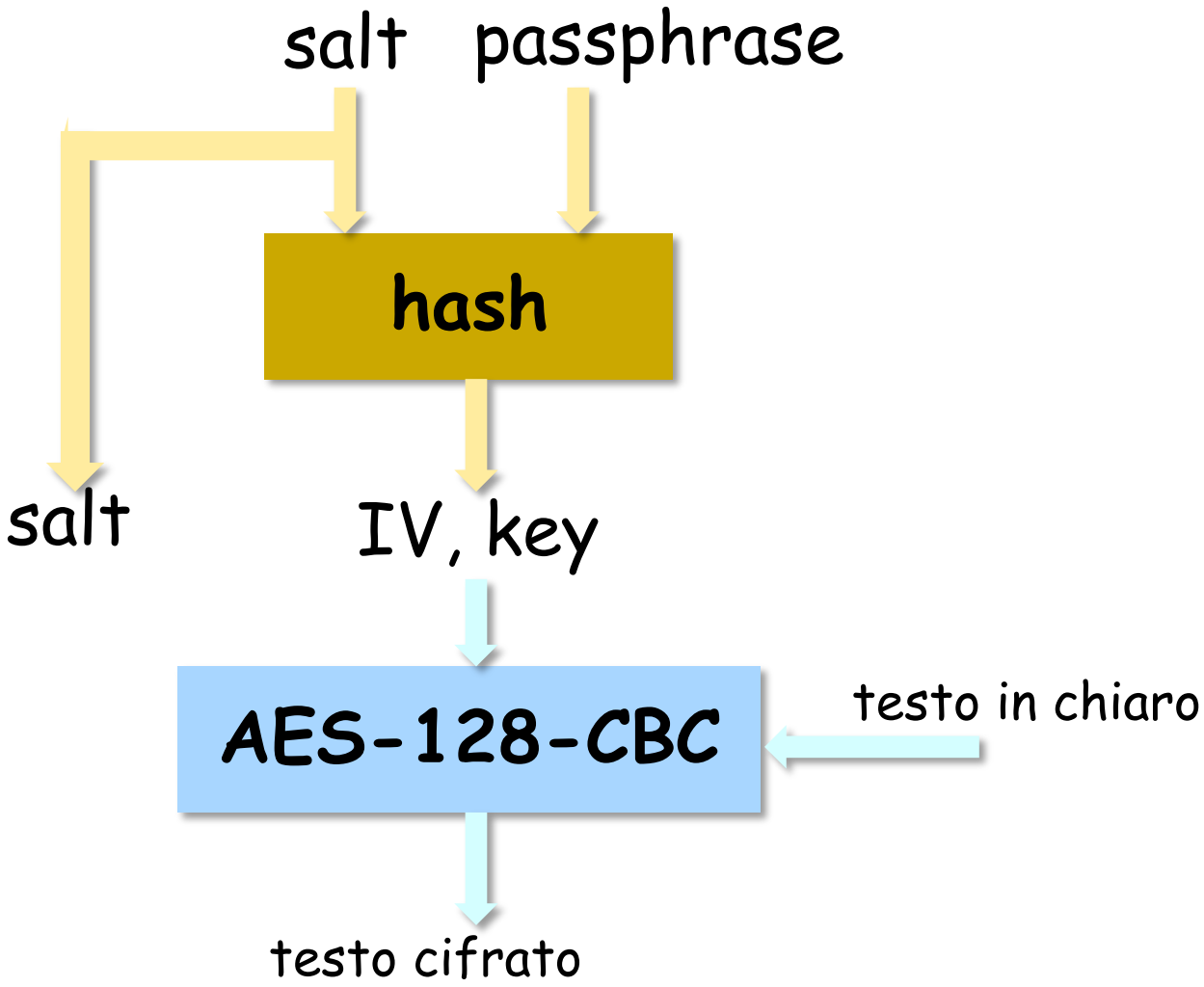
FileCifrato.rtf

```
Salted__^M äïo (ä÷~Å<84>ÑwÛ«áxEB¼º<8f>^GvÂ6CzÌ<8f>iT<95><8c>^Z-}{^Aü^Qà-^W^K^HùÞ
<95>: <94>1^PUé'þ^Y<89>Z^NÙG¯÷ÛëW¦Þül1M<92>^Ag®<9b><82>õ1^E<85>NU^\^G<83>ðÍÁ®^i¨
% }^Yv^Xg!qó^B¤^K»mh¯<8a>ßó<9d>èÜ<84>Ea¶Å3<9e>ï¬<93><95>°^¨y<99>P6º^L^\£e<88>JU
^@&º^O<89><93>S <99>ú^[ÐÆÉÜ<9d>±Ø^E»æ¦<8d>Pðw°×ú^AÐÊ¥R$Úâà°<99>·-ÆñI^\<85>^M<8e>
@,+ÖÍÀu(hï<9c>\^Hs,^L¤ý^F<9c>gÞ9kÅ}#h é«^H<86>¥aÔxí?;l^S£Ç<90>y¤
+.î<88>ZT=b<9d>2ÿ<92>q<8b>¬1[à¢^Oà^W^Ue<90>Ü_EKñ^X^Q÷Ø^@$ÜöI^@t^Yåó`TO<9c>é]x^@È
LB^U;gÅ<9e>-{m^\Ô¤«<8a>^G§n,<98>
LÈ^BÈj--^F8/^A!Ú8^^^]^UÖ*¶èX7±^H<87><85>S§¶\C^[<95>^[óãþGc^YéD<89><9f><90>IÎ<8c>
<87>{^SÎ=K^P<93>¨J0`Å<9f>^FDJ%<94>ñµ^L^?æZü#î.öÝ<96>\8<9b>¸^LùÁ1f7T0Ñh:}ï^VoWþ^G
^?HöÞ<99>âÐ<97>^Sôò³ïCfõöÒNÝ_£îÈI&YÀÔüØ>Ëw^M}.°L·@4^P^JÜ`ò*ÿY^MI"1á^C<8d><8e>F<9
5><92>©[!qmi^K^Sõ<9c><89>À<8c><97>ær¢+<90>Öf{ÞX;<91>^Tc^G6à^]áh<8a>yY´A*^[^[cõD#
°<8b>Ô^3ý6ý^R´^Q:^L65mÏ<86>î?U,Nê^@`ULYäMz#^\5OOÿD^A^?§J7<92>ëo,u<8f>>ýÃ~~LñxºD^
HV^\¢^M<91>-®&hð®V
<9a>øc=ûÁ^[rä}Â[½@\ÖUâý^Pæ½ùÁ<89>^BÏGÞf<97>Ûwó3Õ¡õ¤<83>½³QÚh<83>£4=^Oh®Æ<96>ì<8d
>9)<8c><80>ýùè<97>Nð,<95>;^\ÓÚ_P§Z<99>,*à=ÛU<94>ñã¢>Ü?Z®2Ü@$ql^G<83>çÂÏ^B^R&ºau<
93>¿<88>a^Y²w^VtèºLCF² %ÙÞéZZ^CuLaëfs×^Zm3Õâ^Fø<93>â-Ò¡<98>^TÛ&£|^Hi^C^U_Ï<8c>¡ô
^\¤ÿÜ-^^ã<81><8e><99>-ã1<9a>on:CpÄ{¼¡{2sì{h<8a>¥U<82>Ô^K¤]ÝCj<89>0YuÒ ¡ûLº7Ô<9d>
```

enc con passphrase
(derivazione chiave)



enc con passphrase
(derivazione chiave e cifratura)



Generare chiavi da password

- PBKDF2 (Password-Based Key Derivation Function 2)
  - PKCS #5: Password-Based Cryptography Specification, Version 2.0
  - Pubblicato come RFC 2898
  - Usa HMAC più volte ed un salt per derivare una chiave
  - PBKDF1 genera chiavi solo a 160 bit

NIST Special Publication 800-132,
Recommendation for Password-Based Key Derivation, December 2010
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf

Cifratura Simmetrica in OpenSSL

(Cifratura e Codifica Base 64)

Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura ché la diritta via era smarrita. Ahi quanto a dir qual era è cosa dura esta selva selvaggia e aspra e forte che nel pensier rinova la paura! Tant'è amara che poco è più morte; ma per trattar del ben ch'i' vi trovai, dirò de l'altre cose ch'i' v'ho scorte.

FileInChiaro.rtf

Cifratura e Codifica Base 64

```
openssl enc -aes-256-cbc -in FileInChiaro.rtf -out FileCifratoB64.rtf -e -base64 -pass
pass:P1pp0B4ud0
```

FileCifratoB64.rtf

U2FsdGVkX18LBDbd1sxWx4xZGaTlB7dSwmJ1xAcgLqkpsRl3jhY3mLdnBzJOmck3d2ZDhtGh8siGPmuuA2NF0dl1YdSf/zAK1Bo
+90odha4e9r7f4qtUNfHmNlWJeQabMmcd50omOplXYDhCROXiG490nTxSMcOtvGNxTIJrqHUDqQ8xVBMnb0dafpTU+229dV/
du6pwLCh9IKXDQIAvsPScHbOoZyBDxmvgcI6kbPrEeqL2M+/0fLaNumZWPnd4QwpFYHZKHb+UPX0p1BhGQ77M8GcVBcGeGarVE/
BeAKOcyo78UhQ9BvNclNywt3VlquYVVBRQDZO8dGTLDLe6UUgSxblucELY19hRiIhb+HdgwjJKpdx
+xHobksl69n9uTwEO8TzUsKkLOg3LtODAizZdXsidJX0+ZT76ijW7zkwufFUl8zYY1C6+RRqSNqiUB5VIXzUDlFxkOQ4JyN2mziKSQPv840o0+
C4ShdWPp5eCXIoRA3Ar7bx4AO3AyzzP0nW1kHbCESddSFYho0tS0q4qGy0s4CvKabjch1yre+HZo+GpwtqCZK0Yxy11Isc2Ft2MmRm6X//
QfKwdYhiMa0HhPpmGMjZgWP2dg/
+HmIbKR8Mw41mAc3NoogBy4YbXYjopUdFrtadsoGUnQmpr5uHDiks9KdxY7ZogNy2G5K8avSkaMj1sPHT9pBS23SrV9FYorg9AVZlIigYPuVeX
9StNStP4/NzCeYXe/4fO6Uz8W/nLGgpEJ1GYwu1qR9HtdwVvajvQnaqq0HV9sQcoLyvcaZUTrPLJ3+bFu3SvA8ha+TPQEzwIdXqxePfGQE/
opdGJzmALfk9uIOu5awdDBYUzXiB8LMk0YiInDZrQ5BLfnMzK5P80SH4zrhZ+rdHCAQ/QMyTJeb7BIF+HLElfOu1Z/czUQQcmEd
+A8bUD7WrfJHJ/UUZhlCtt/sCUArfXThzRNoIueRLPXJlKdIilbK8VyW/Ei7fCycrmPtQB4/xmstCSMtQTe
+P0AKa6xHda1WsEPcPeOx04KmsxPtFFLbVP7W+wExgWZLgrzImN6WQvJo8h4mJ8zsoIeizMHgSjq+oEAN1W7ou8TNZUyvURtg==

Cifratura Simmetrica in OpenSSL

(Decifratura)

FileCifratoB64.rtf

U2FsdGVkX18LBDbd1sxWx4xZGaTlB7dSwmJ1xAcgLqkpsRl3jhY3mLdnBzJOmck3d2ZDhtGh8siGPmuuA2NF0dl1YdSf/
zAK1Bo
+90odha4e9r7f4qtUNfHmNlWJeQabMmcd50omOplXYDhCROXiG490nTxSMcOtvGNxTIJrqHUDqQ8xVBMnb0dafpTU
+229dV/du6pwLCh9IKXDQIAvsPScHbOoZyBDxmvgcI6kbPrEeqL2M+/0fLaNumZWPnd4QwpFYHZKHb
+UPX0p1BhGQ77M8GcVBcGeGarVE/BeAKOcyo78UhQ9BvNclNywt3VlquYVVBRQDZO8dGTLDLe6UUgSxblucELY19hRiIhb
+HdgwjJKpdx
+xHobksl69n9uTwEO8TzUsKkLOg3LtODAizZdXsidJX0+ZT76ijW7zkwufFUl8zYY1C6+RRqSNqiUB5VIXzUDlFxkOQ4JyN2mz
iKSQPv840o0+C4ShdWPp5eCXIoRA3Ar7bx4AO3AyzzP0nW1kHbCESddSFYho0tS0q4qGy0s4CvKabjch1yre+HZo
+GpwtqCZK0Yxy11Isc2Ft2MmRm6X//QfKwdYhiMa0HhPpmGMjZgWP2dg/
+HmIbKR8Mw41mAc3NoogBy4YbXYjopUdFrtadsoGUnQmpr5uHDiks9KdxY7ZogNy2G5K8avSkaMj1sPHT9pBS23SrV9FYorg9
AVZlIigYPuVeX9StNStP4/NzCeYXe/4fO6Uz8W/
nLGgpEJ1GYwu1qR9HtdwVvajvQnaqq0HV9sQcoLyvcaZUTrPLJ3+bFu3SvA8ha+TPQEzwIdXqxePfGQE/
opdGJzmALfk9uIOu5awdDBYUzXiB8LMk0YiInDZrQ5BLfnMzK5P80SH4zrhZ+rdHCAQ/QMyTJeb7BIF+HLElfOu1Z/
czUQQcmEd+A8bUD7WrfJHJ/UUZhlCtt/sCUArfXThzRNoIueRLPXJlKdIilbK8VyW/Ei7fCycrmPtQB4/xmstCSMtQTe
+P0AKa6xHda1WsEPcPeOx04KmsxPtFFLbVP7W+wExgWZLgrzImN6WQvJo8h4mJ8zsoIeizMHgSjq
+oEAN1W7ou8TNZUyvURtg==

Decifratura di file codificato in Base 64

```
openssl enc -aes-256-cbc -in FileCifrato.rtf -out FileDecifrato.rtf -d -base64 -pass
pass:P1pp0B4ud0
```

Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura ché la diritta via era smarrita. Ahi quanto a dir qual era è cosa dura esta selva selvaggia e aspra e forte che nel pensier rinova la paura! Tant'è amara che poco è più morte; ma per trattar del ben ch'i' vi trovai, dirò de l'altre cose ch'i' v'ho scorte.

FileDecifrato.rtf

Cifratura Simmetrica in OpenSSL

(Cifratura e Codifica Base 64 con password da file)

Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura ché la diritta via era smarrita. Ahi quanto a dir qual era è cosa dura esta selva selvaggia e aspra e forte che nel pensier rinova la paura! Tant'è amara che poco è più morte; ma per trattar del ben ch'i' vi trovai, dirò de l'altre cose ch'i' v'ho scorte.

FileInChiaro.rtf

Cifratura con password letta da file e codifica Base 64

```
openssl enc -aes-256-cbc -in FileInChiaro.rtf -out FileCifratoB64.rtf -e -base64 -pass
pass:password.txt
```

FileCifratoB64.rtf

U2FsdGVkX18hL9rC2FLmVrrlpi8xl6/d02wFVPnlwMvNU96sAh5kILpsTmKr/
sf0N5fiH7OwijixKscWQXacxwB058ow1cS6YmEL88mpwXHZVTYUr5A0jbU+t9UgAVQN5YIrw7gq3Xohl+0xgVOMY4YRq3N/
kU++S3yUxt73iM6x/iXGd1LSPoMf3mP84ZXLOUOUYDXxogGr9iR9GdxKsM/
dkAR7TWsWhqSqY0ATHGTkAof46qemlnhSxuWz1Sq6GskOKBDB1f5sCTxaRqZG3/
u88pVmbRRUJ0J0R7zWfBtkGRrat8a00U6re7jiMaHC6PpMt3MWD6EQYmUiEqIjKkP
+VpYy5egwZdBBCUuvu8+b2M2n16wuRyfkstNrYkD9scYowwoXYs26yNKQQSD7fMRZ/
nmt2evFIPn4NM7B95lgbck40aDHqAY6l/+G/kJQfPCNQd5X2wRGL1mVTrBUvJ/
BI8ZuockffjDAf9tj6efUhdgJbCa0KaJHdbysjGa2dDHlc1rOYu8slvDvufkhCG8UcAfOmQ73M6b0G01285lZNQRYuvw0zOf9vw
4PnWb6wVxWHNMMyPn4F3eJrtv5C2pN9RQON/VPfByWEN/E8n1dtUTpF/
VCS06MHk5hynVIgTpaKWIcerCMcEgU3ucW6NRmgI5DboguGJReFxPAkGGcumgi3PwpMd6wVi8vR42rn6uyztfKpmwf9MpQD
xsSBn5Fk7oRsv5aP6aCWGg2n0U3Ah7chbDBpljmdcLjcUrrVuEKqa/uN8vH72LLwBHLgKfSjQweu4R4nTTzXdkPgDQuOf9y
+xRt2gRzx/FIRY8d3klSMvzSiXSE1Gc2KWo2ATvxrlB+fq0Jeq2Pou3zGEVUchyBlE2VNfONMjuc3O7/
qvJjK46rrBRNiC3sBQq1eU28XZPHPWBSEL2BObAR0G6UqBi2yX+QBp9DH0fZ6uiKcai0FmKS9nPSSePmJO18qXhsBnUVDt
+AcedtVv/9tklaBrXt1Ff41HFxKURqwvJ2tFb2xVXkXUUyxBAYhpixnMNq6tkgScR/F5RzMGdbAY2V
+jOg0Q4pggjvOH1Vjan3N9gV60PqdH51IAhY80HXpg==

Cifratura Simmetrica in OpenSSL

(Decifratura con password da file)

FileCifratoB64.rtf

```
U2FsdGVkX18hL9rC2FLmVrrlpi8xl6/d02wFVPnlwMvNU96sAh5kILpsTmKr/
sf0N5fiH7OwijixKscWQXacxwB058ow1cS6YmEL88mpwXHZVTYUr5A0jbU+t9UgAVQN5YIrw7gq3Xohl+0xgVOMY4YRq3N/
kU++S3yUxt73iM6x/iXGd1LSPoMf3mP84ZXLOUOUYDXxogGr9iR9GdxKsM/
dkAR7TWsWhqSqY0ATHGTkAof46qemlnhSxuWz1Sq6GskOKBDB1f5sCTxaRqZG3/
u88pVmbRRUJ0J0R7zWfBtkGRrat8a00U6re7jiMaHC6PpMt3MWD6EQYmUiEqIjKkP
+VpYy5egwZdBBCUuvu8+b2M2n16wuRyfkstNrYkD9scYowwoXYs26yNKQQSD7fMRZ/
nmt2evFIPn4NM7B95lgbck40aDHqAY6l/+G/kJQfPCNQd5X2wRGL1mVTrBUvJ/
BI8ZuockffjDAf9tj6efUhdgJbCa0KaJHdbysjGa2dDHlc1rOYu8slvDvufkhCG8UcAfOmQ73M6b0G01285lZNQRYuvw0zOf9vw
4PnWb6wVxWHNMMyPn4F3eJrtv5C2pN9RQON/VPfByWEN/E8n1dtUTpF/
VCS06MHk5hynVIgTpaKWIcerCMcEgU3ucW6NRmgI5DboguGJReFxPAkGGcumgi3PwpMd6wVi8vR42rn6uyztfKpmwf9MpQD
xsSBn5Fk7oRsv5aP6aCWGg2n0U3Ah7chbDBpljmdcLjcUrrVuEKqa/uN8vH72LLwBHLgKfSjQweu4R4nTTzXdkPgDQuOf9y
+xRt2gRzx/FIRY8d3klSMvzSiXSE1Gc2KWo2ATvxrlB+fq0Jeq2Pou3zGEVUchyBlE2VNfONMjuc3O7/
qvJjK46rrBRNiC3sBQq1eU28XZPHPWBSEL2BObAR0G6UqBi2yX+QBp9DH0fZ6uiKcai0FmKS9nPSSePmJO18qXhsBnUVDt
+AcedtVv/9tklaBrXt1Ff41HFxKURqwvJ2tFb2xVXkXUUyxBAYhpixnMNq6tkgScR/F5RzMGdbAY2V
+jOg0Q4pggjvOH1Vjan3N9gV60PqdH51IAhY80HXpg==
```

Decifratura di file codificato in Base 64, con password letta da file

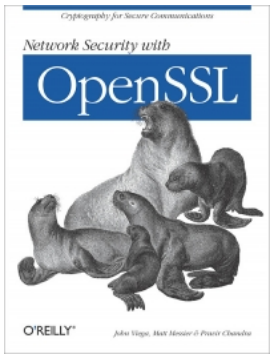
```
openssl enc -aes-256-cbc -in FileCifratoB64.rtf -out FileDecifrato.rtf -d -base64 -pass
pass:password.txt
```

Nel mezzo del cammin di nostra vita mi ritrovai per una selva oscura ché la diritta via era smarrita. Ahi quanto a dir qual era è cosa dura esta selva selvaggia e aspra e forte che nel pensier rinova la paura! Tant'è amara che poco è più morte; ma per trattar del ben ch'i' vi trovai, dirò de l'altre cose ch'i' v'ho scorte.

FileDecifrato.rtf

Bibliografia

- Network Security with OpenSSL
  Pravir Chandra, Matt Messier and John Viega (2002), O'Reilly
  - Cap. 2.1 e 2.3



- Documentazione su OpenSSL
  - https://www.openssl.org/docs/

OpenSSL
Cryptography and SSL/TLS Toolkit

Domande?