mozilla clubs
Cagliari

WEBATECA

OTTAVO LABORATORIO
CRITTOGRAFIA ASIMMETRICA

Edoardo Viola
@edovio
Cagliari, 21/01/2017

WEBATECA DEL MEDITERRANEO

LA CRITTOGRAFIA

COSA SIGNIFICA

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

LA CRITTOGRAFIA

METODO PER RENDERE UN MESSAGGIO “OFFUSCATO” IN MODO DA NON POTER ESSER LETTO A PERSONE NON AUTORIZZATE

TRACCE DEI PRIMI METODI DERIVANO DA PRIMA DEGLI ANTICHI ROMANI

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

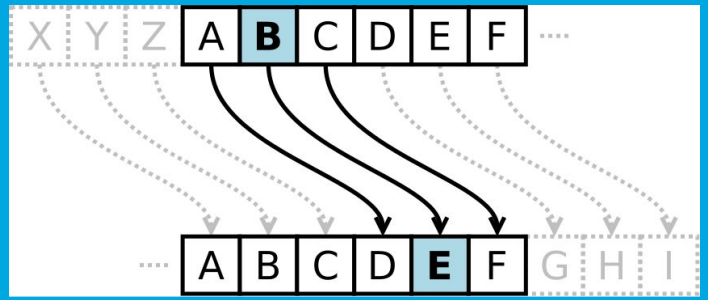
MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

LA CRITTOGRAFIA

CIFRARIO DI CESARE

Cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto.



Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

LA CRITTOGRAFIA

La crittografia è una parte fondamentale dei principali sistemi di comunicazione moderni e permette direttamente o indirettamente di poter proteggere la condivisione delle informazioni, WEB incluso.

(Prossimamente vedremo come viene applicata nel Web)

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

LA CRITTOGRAFIA

SIMMETRICA

ASIMMETRICA

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

LA CRITTOGRAFIA

SIMMETRICA

Definita anche come a Chiave Privata rappresenta un metodo semplice per cifrare testo in chiaro dove la chiave di crittazione è la stessa di decrittazione

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

LA CRITTOGRAFIA

ASIMMETRICA

Definita anche come a Chiave Pubblica o a Chiave Pubblica/Privata, rappresenta un metodo per cifrare testo in chiaro attraverso l'utilizzo di due chiavi:

- Chiave Pubblica (Può essere distribuita pubblicamente)
- Chiave Privata (Personale e segreta)

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

LA CRITTOGRAFIA

ASIMMETRICA

Definita anche come a Chiave Pubblica o a Chiave Pubblica/Privata, rappresenta un metodo per cifrare testo in chiaro attraverso l'utilizzo di due chiavi:

- Chiave Pubblica (Può essere distribuita pubblicamente)
- Chiave Privata (Personale e segreta)

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA

COME FUNZIONA

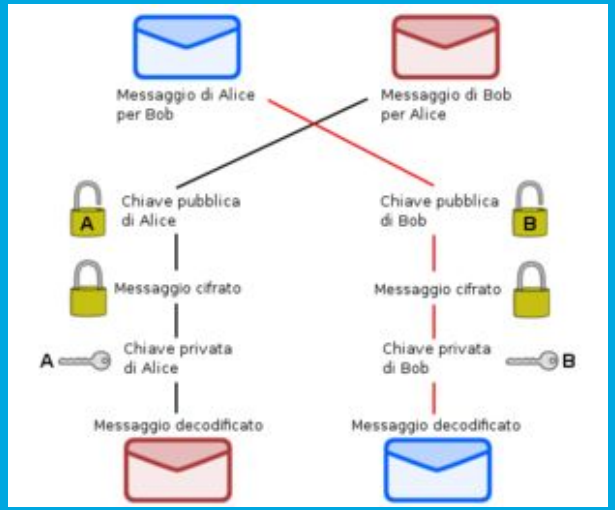
Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA



Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA

Ogni utente genera la sua coppia di chiavi
e diffonde la propria chiave pubblica

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA

Ogni volta che invio un messaggio ad un destinatario sfrutto la sua chiave pubblica per cifrarlo.

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA

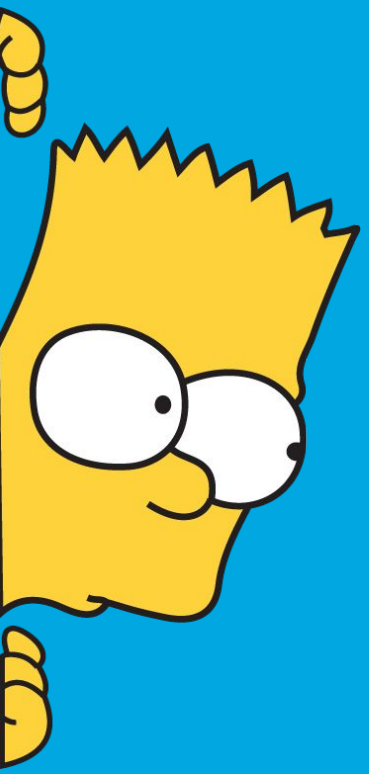
Solo il destinatario in possesso della corretta chiave privata può decifrare il messaggio e poterlo leggere

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO



DOMANDE ?

Edoardo Viola
@edovio
Cagliari, 21/01/2017

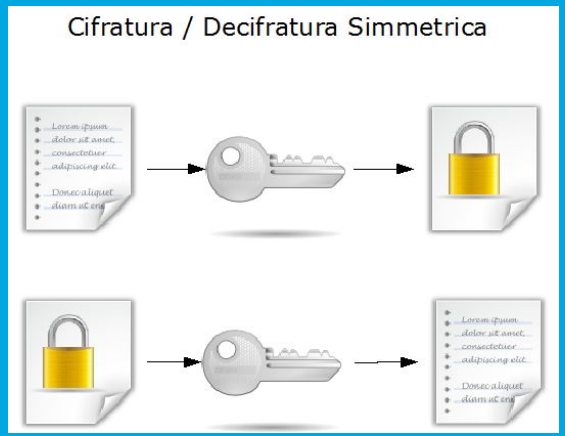
mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA

GIOCHIAMO CON LA CRITTOGRAFIA



Edoardo Viola
@edovio
Cagliari, 21/01/2017

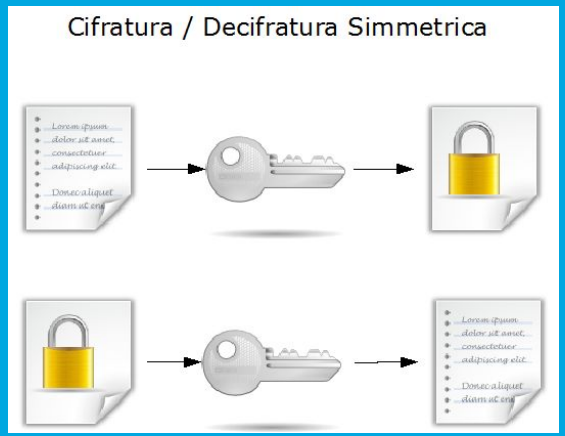
mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA

ACCEDERE AL SEGUENTE SITO:
https://codemoji.org
SCRIVERE UN MESSAGGIO E SCRIVERE IL LINK IN UN POST-IT E CONSEGNARLO ALLA VOSTRA CHIAVE PUBBLICA.



Edoardo Viola
@edovio
Cagliari, 21/01/2017

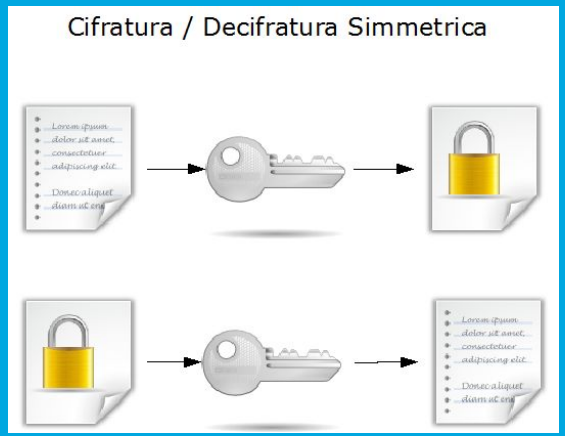
mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA

TEMPO MASSIMO 20 MINUTI

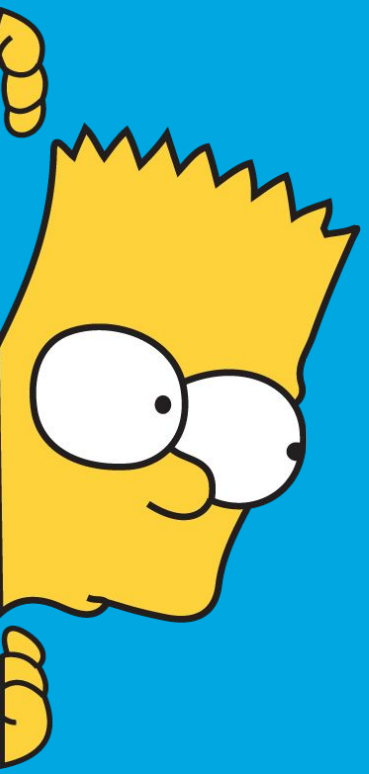


Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO



DOMANDE ?

Edoardo Viola
@edovio
Cagliari, 14/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

LA CRITTOGRAFIA

CRITTOGRAFIA E EMAIL

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

PROTONMAIL

ProtonMail

Servizio Email con crittografia point-to-point open Source e gratuito

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

ESTENSIONI

ENCRYPTED COMMUNICATION
Estensione che permette di cifrare in chiave pubblica qualunque messaggio inviato con il Browser

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

ESTENSIONI

ENIGMAIL

Estensione per Mozilla Thunderbird per integrare su qualsiasi Email la cifratura a chiave pubblica

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

TUTORIAL ENIGMAIL

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

ENIGMAIL

INSTALLARE ENIGMAIL

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA

INSTALLARE SUL PROPRIO COMPUTER CON THUNDERBIRD ENIGMAIL

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CHIAVE PUBBLICA

TEMPO MASSIMO 30 MINUTI

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

CONSIDERAZIONI

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

RIEPILOGO

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO

WEBATECA DEL MEDITERRANEO

A SABATO PROSSIMO!!!

Edoardo Viola
@edovio
Cagliari, 21/01/2017

mozilla clubs
Cagliari

MEDIATECA DEL MEDITERRANEO