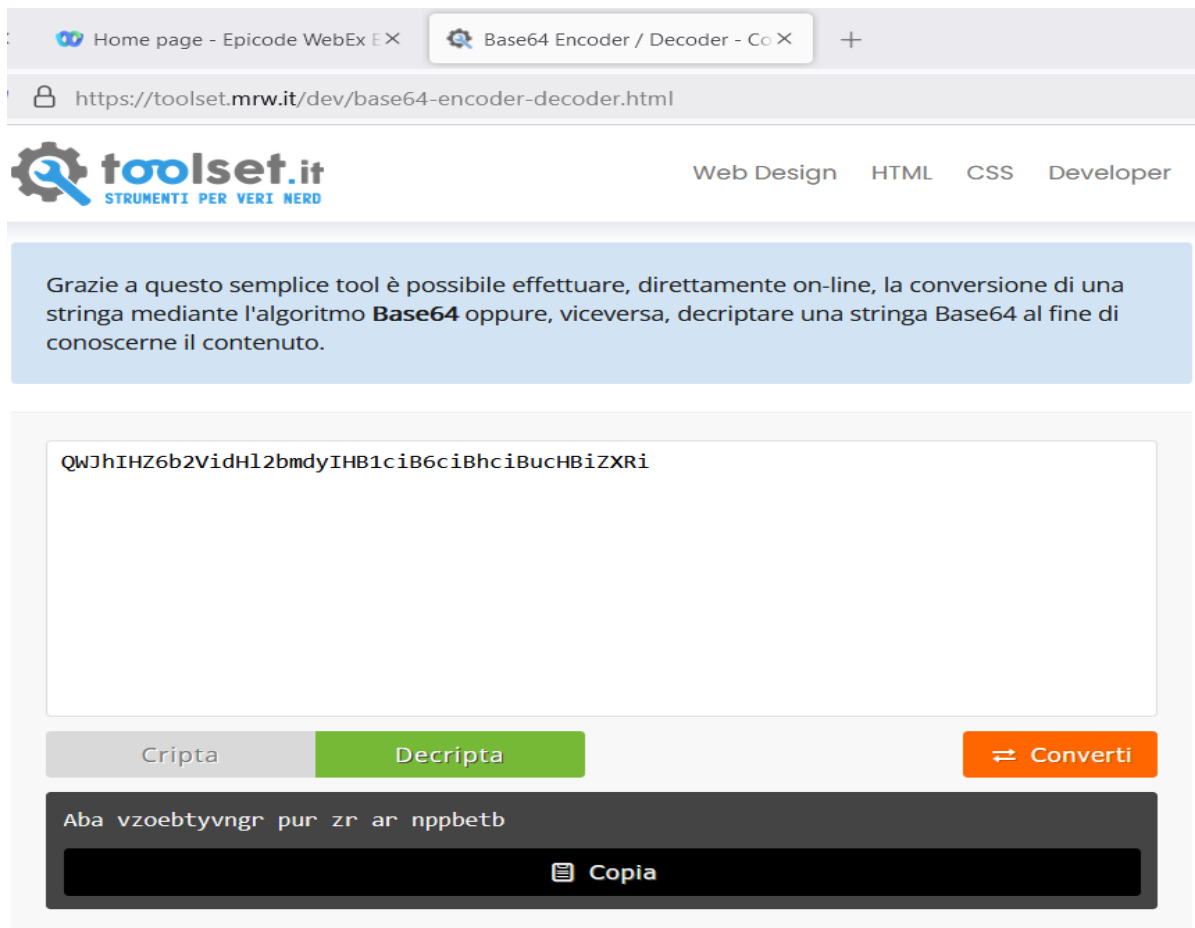


Laboratorio 12/12/2024 S3-L4

Nel laboratorio odierno innanzitutto dobbiamo decifrare la seguente riga di testo:

QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZX Ri

Utilizzando dei tool online andiamo prima a decifrare in base64 e otteniamo il testo:



The screenshot shows a web browser window with two tabs: 'Home page - Epcode WebEx E X' and 'Base64 Encoder / Decoder - Co X'. The address bar shows the URL 'https://toolset.mrw.it/dev/base64-encoder-decoder.html'. The page header includes the 'toolset.it' logo with the tagline 'STRUMENTI PER VERI NERD' and navigation links for 'Web Design', 'HTML', 'CSS', and 'Developer'. A light blue informational box states: 'Grazie a questo semplice tool è possibile effettuare, direttamente on-line, la conversione di una stringa mediante l'algoritmo **Base64** oppure, viceversa, decriptare una stringa Base64 al fine di conoscerne il contenuto.' Below this is a large text input area containing the Base64 string 'QWJhIHZ6b2VidHl2bmdyIHB1ciB6ciBhciBucHBiZX Ri'. At the bottom, there are three buttons: 'Cripa' (disabled), 'Decripa' (active), and 'Converti' (orange). Below the buttons, a dark grey box displays the decoded text 'Aba vzoebtyvngr pur zr ar nppbetb', and a 'Copia' button is located at the bottom right of this box.

Aba vzoebtyvngr pur zr ar nppbetb

A questo punto utilizziamo il cifrario di Cesare ed effettuiamo vari tentativi fino allo spostamento di 13 lettere ed otteniamo il messaggio:

https://kryptos.altervista.org/cesare/



Cifrario di Cesare

Inserire un numero da 0 a 25:

Aba vzoebtyvngr pur zr ar nppbetb

Non imbrogliate che me ne accorgo

Una breve spiegazione sull'uso di questo cifrario la trovi [qui](#)
Una versione da stampare e gratuita invece la trovi [qui](#).

Non imbrogliate che me ne accorgo

ESERCIZIO BONUS:

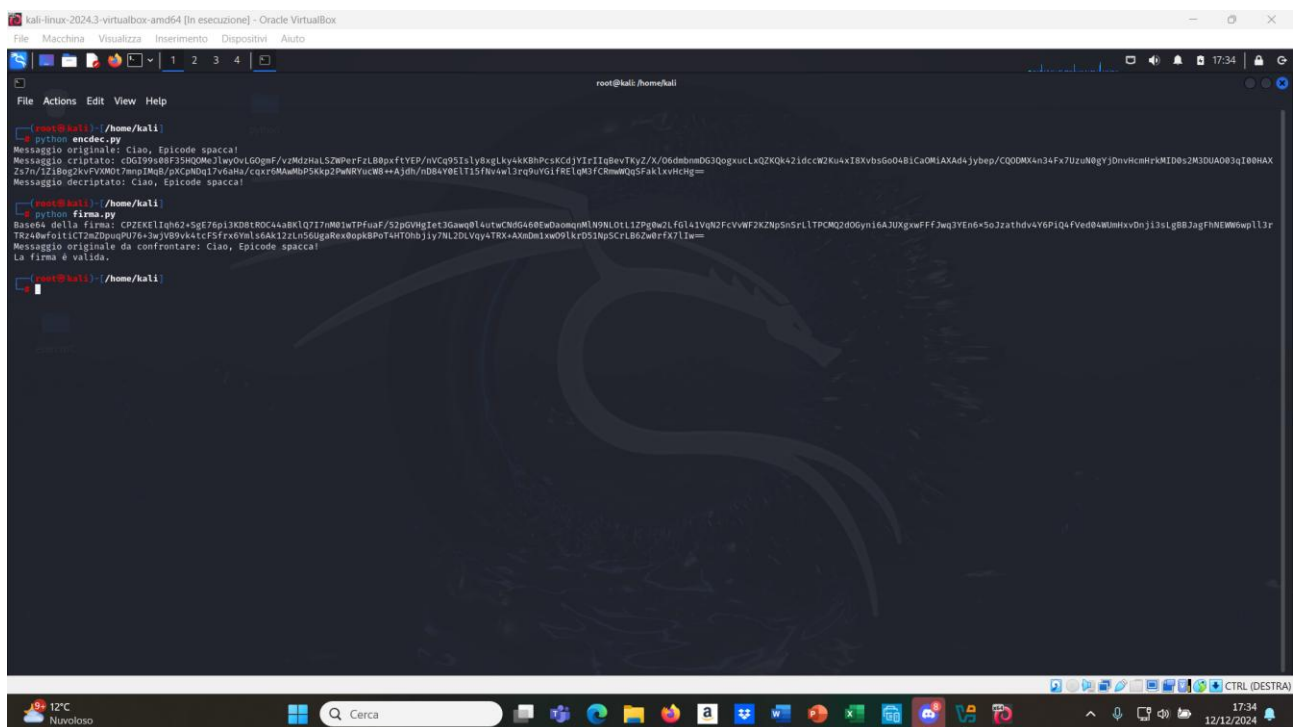
Criptazione e Firmatura con OpenSSL Python:

Obiettivi dell'esercizio:

- Generare chiavi RSA.
- Estrarre la chiave pubblica da chiave privata.
- Criptare e decriptare messaggi.
- Firmare e verificare messaggi.

Strumenti utilizzati:

- OpenSSL per la generazione delle chiavi.
- Libreria cryptography in Python.



```
kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

root@kali:~/home/kali

root@kali:~/home/kali# python3 encdec.py
Messaggio originale: Ciao, Epicode spacca!
Messaggio criptato: cDGI99908F35HQMeJwyOvLGOgHf/vzMdZHaLS2WheFzLB8pxfYEP/nVCq95Isly8gLykK8BpCsKCdJY1rI1qBevTkyZ/X/06dmbnmDG3QgucLxQZKQk421dcw2Ku4x18XvbsGo04B1CaOM1AXAd4Jybep/CQODMXAn34Fx7UzuN8gYJ0nvHcmHrKMI08s2K3DUAO83q188HAX
Zs7u/1218g2xvFVMO77mqJ3MaB/pXCPmQd17v6aha/cqxr0MawMDP5Kxp2PwRRYucW8++A3dH/nD84Y0EL115fNv4w13rq9uG1fRElqQ3FCRmWQ5FakLxvHCHg==
Messaggio decriptato: Ciao, Epicode spacca!

root@kali:~/home/kali# python3 firma.py
Base64 della firma: CPZEK1Iqh62+5gE76pi3K08tROCA4abKlQ7I7nM01wTPfuaF/52p0VHgIet3Gawq014utwCn05A68EwDaomqnM1N9NLO1L1ZPg0w2Lfo141VqN2FcVWF2KZn5nSrl1TPCM2d0Gyn16AJUXgwxFF7wq3Yen6+5o3zathd4vYGP1Q4FVed84WmHxvDn3i3sLg8B3agFNEW9wep113f
R2x4w4fo1c1C7n2p0uqU76+3w3jv09v4tCf5Fxe0vls6Ak12ZLn50gaRex8op48P0t4HT0b3jy7NL2DLVqy+TRX+AX0m1xw09LkrD51Np5CfL86Zw0fFX7Liw==
Messaggio originale da confrontare: Ciao, Epicode spacca!
La firma è valida.

root@kali:~/home/kali#
```