Crittografia con Python

Corso introduttivo
Marzo 2015

Con materiale adattato dal libro “Hacking Secret Cypher With Python”
di Al Sweigart (http://inventwithpython.com/hacking/index.html)

Prof. Alessandro Bugatti

Nascondere segreti

- Fin dai tempi più remoti c'è sempre stato interesse a mantenere dei segreti, che dovevano essere conosciuti soltanto da alcune persone

"Un segreto è il tuo prigioniero:

se lo lasci fuggire sarai il suo prigioniero"

Nascondere segreti

- Persone interessate: militari, corpo diplomatico, scrittori di diari e amanti
- Gli esempi più remoti di tentativi di tenere celata un'informazione possono trovarsi nelle *Storie* di Erodoto (V secolo a.C.), nelle quali narra dell'invasione persiana in Grecia

Steganografia

- Dal greco *steganòs* (coperto) e *gràphein* (scrittura).
- I messaggi vengono coperti in modo che non possano essere visti o, anche se visti, non siano interpretati come tali.
- La steganografia appare prima della crittografia perchè si basa su stratagemmi “furbi” per coprire il messaggio

Esempi di steganografia

- Dalle Storie di Erodoto:
  - il messaggio veniva scritto su un legno il quale veniva poi ricoperto di cera e scambiato così per una tavoletta da scrittura ancora vergine (Demarato).
  - il messaggio veniva scritto sulla testa rasata del messaggero, gli si facevano crescere i capelli (quindi non si aveva fretta...) e poi lo si mandava a destinazione (Istièo).

Altri esempi

- La steganografia è stata usata in tempi più recenti
  - XVI secolo, Giambattista Della Porta e il metodo dell'uovo sodo
  - scrittura con inchiostri simpatici
  - striscioline finissime di seta appollottolate, ricoperte di cera e inghiottite dal messaggero
  - microdot

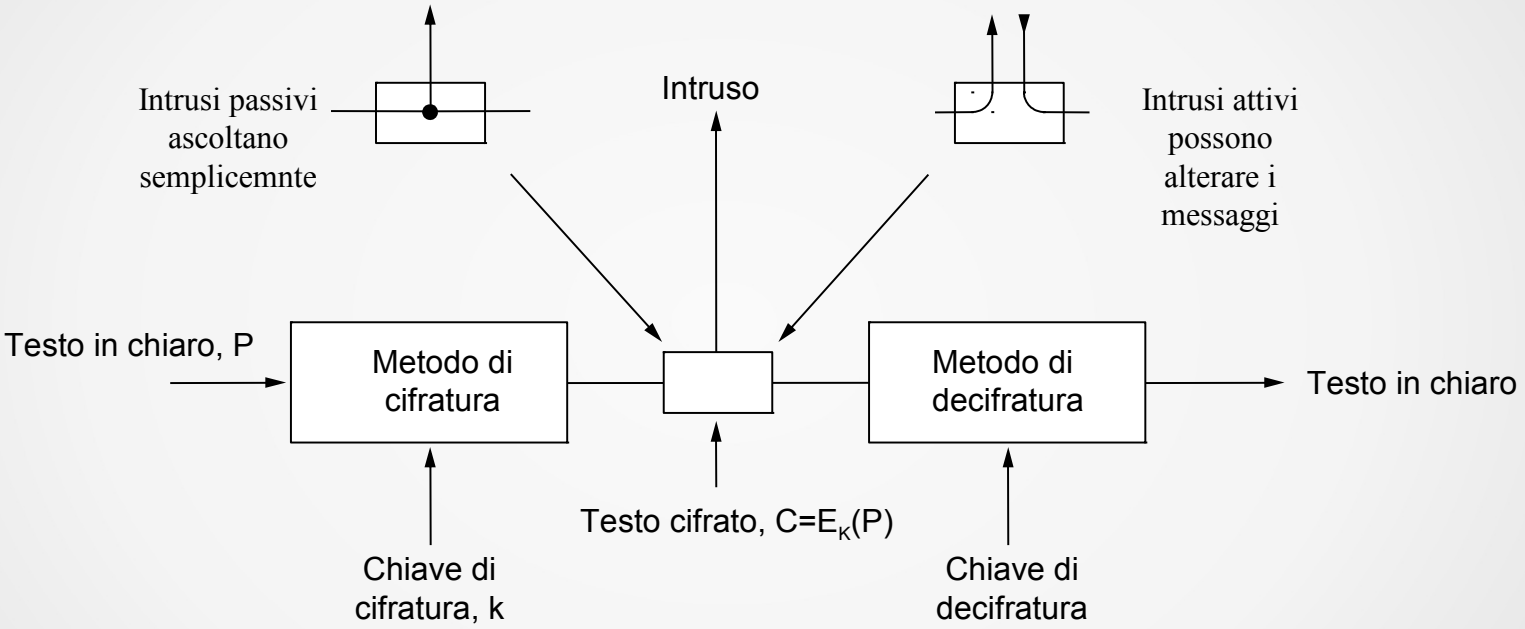
Limiti della steganografia

- Se il messaggio viene visto, tutta l'informazione è immediatamente disponibile
- Per superare questi limiti viene sviluppata la **crittografia**, dal greco kryptòs, che significa nascosto
- Anche la crittografia ha origini antiche

Crittografia: definizioni

- La crittografia tratta dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate a leggerlo.
- La **crittografia** è la controparte della **crittanalisi** ed assieme formano la **crittologia**.

Modello crittografico



Crittografia: terminologia

- **Testo in chiaro (P)**: messaggio da codificare
- **Chiave (K)**: parametro della funzione di cifratura
- **Testo cifrato (C)**: testo cifrato

$C = E_K(P)$ Codifica del testo P usando la chiave K

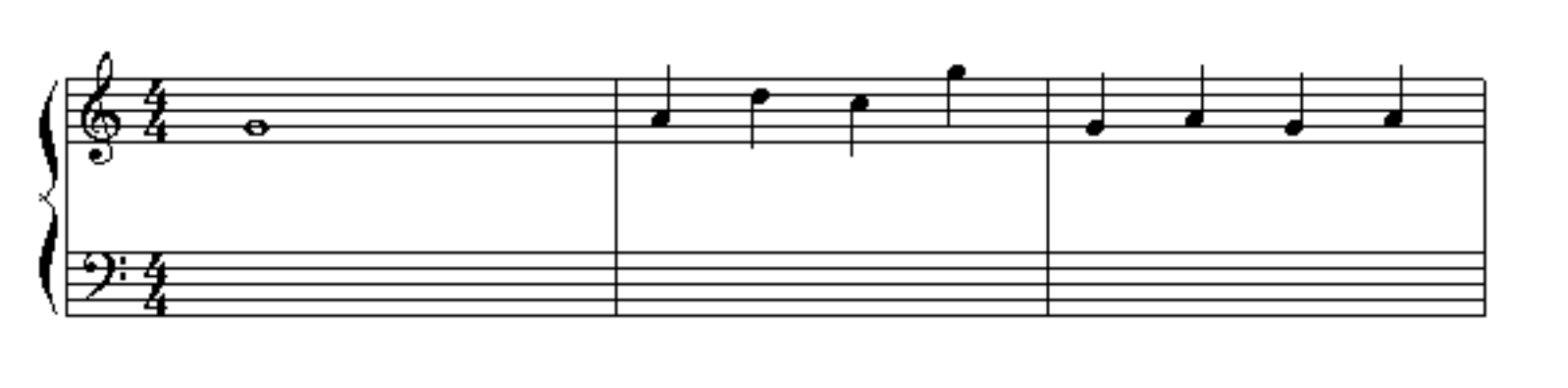
$P = D_K(C)$ Decodifica del testo C usando la chiave K

$$D_K(E_K(P))=P$$

Regola fondamentale (Auguste Kerckhoffs – 1883)

- Si assume che chi voglia violare il codice sia a conoscenza del metodo di codifica usato, ma non della chiave:
  - troppo sforzo per inventare, verificare e installare un nuovo metodo ogni volta che ci si rende conto che non è più segreto
  - pensare che un metodo sia segreto quando effettivamente non lo è può essere molto pericoloso

Esempio



- Metodo di cifratura segreto, nessuna chiave

Cifrari a sostituzione

- Ogni lettera o gruppo di lettere vengono rimpiazzati da un'altra lettera o gruppo di lettere
- Uno dei più vecchi e noti è dovuto a Giulio Cesare: viene effettuato uno "shift" di tre posti per sostituire i caratteri

Cesare ⟹ Fhvduh

Metodo di codifica

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Quante possibili chiavi?
- 26, troppo poche, va bene solo per i Cartaginesi…
- Cosa vuol dire IEDERHQLE?

- Linguaggio interpretato
- Orientato agli oggetti
- Libreria molto vasta
- Multipiattaforma
- Open

www.python.org

Ambiente di sviluppo

- Python è disponibile per ogni piattaforma (Windows, MacOs, Linux, Raspberry ecc.)
- Per questo corso si utilizzerà Portable Python, distribuzione portatile per ambiente Windows, nella versione 3.2.5.1, che comprende al suo interno sia l'interprete che una serie di librerie e strumenti utili (IDLE, Ipython, …) e che ha il vantaggio di non richiedere installazione

http://portablepython.com/

IDLE e IPython

- IDLE è sia un editor per la scrittura di programmi che una shell interattiva
- Ipython è un ambiente con una shell interattiva molto sofisticata, con autocompletamento, command history ecc.
- Useremo l'uno e l'altro a seconda della esigenze, Windows non è l'ambiente ideale ma ce la caveremo

Fondamenti “fondamentali”

- Le variabili si dichiarano senza tipo, che viene inferito dal contesto (e non può cambiare implicitamente)
- L'indentazione non è cosmetica, definisce la struttura del programma
- Le strutture dati come liste, tuple, dizionari ecc sono parte del linguaggio
- Lo so che è un po' poco, vedremo il resto poi...

Primo esempio: codice inverso

- Scopo: vogliamo prendere una stringa e invertirla, un semplice esempio di codice senza chiave
- Useremo l'assegnamento tra stringhe, la concatenazione tra stringhe, la funzione per calcolare la lunghezza di una stringa, il ciclo while e la funzione print per stampare il risultato
- Partiamo con IDLE...
- Facile, vero?

Codice di Cesare in Python

- Importazione di un modulo
- Metodi find e upper per stringhe
- Utilizzo dell'operatore di selezione if
- Utilizzo del ciclo for e dell'operatore in
- Utilizzo del modulo pyperclip
- Torniamo a IDLE...

Cifrari a sostituzione

- Piccolo miglioramento: sostituzione monoalfabetica al posto della traslazione
- Al posto di 26 tentativi il crittoanalista ne deve fare 26! (circa 4×10^{26} che è un numero molto grosso): sembra buono

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	Z	X	C	H	J	K	F	M	S	Q	R	G	B	N	L	I	O	V	A	W	E	D	T	Y	U

Complessità computazionale

- Supponendo di avere un computer che esplora un milione di possibilità al secondo

Numero di possibilità	**Tempo impiegato**
26	0,000026 sec.
1 milione	1 sec.
10^{26}	270 milioni di Eu*
10^{38}	2,7 milioni di milioni di Eu*

*Eu = età stimata dell'Universo

E adesso tocca a voi...

- Per casa provare a produrre un cifratore a sostituzione
- Se funziona prendere un file con del testo italiano, sufficientemente lungo, e cifrarlo con una chiave segreta
- La prossima volta vedremo come attaccarlo...