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

Cifrari a trasposizione

- A differenza di quelli a sostituzione non trasformano le lettere ma le riordinano

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Testo in chiaro

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Testo cifrato

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Cifrari a trasposizione

- Per verificare di essere in presenza di un cifrario a trasposizione basta verificare la statistica delle lettere che non viene alterata
- Bisogna poi capire su quante colonne è stata fatta la trasposizione: si fanno delle supposizioni su parole probabili
- Si vede quale delle $k(k-1)$ colonne danno la migliore corrispondenza dei digrammi

Esempio

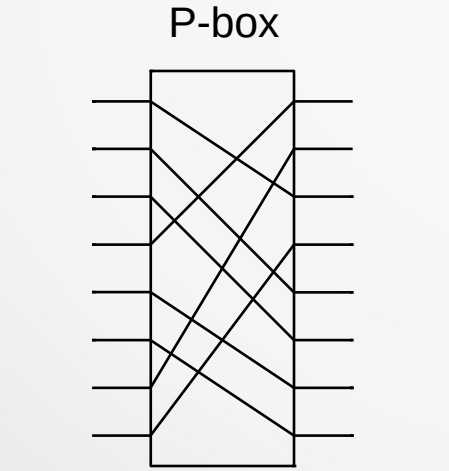
- Supponiamo di sapere che compaia la parola *milliondollars*
- Supponendo varie lunghezze si trova quella corrispondente all'apparizione delle varie parti della parola avvolta su se stessa (con lunghezza 8 si troverebbero MO, IL, LL, LA, IR e OS)
- Si procede permutando le colonne e analizzando la frequenza dei digrammi

Algoritmi moderni

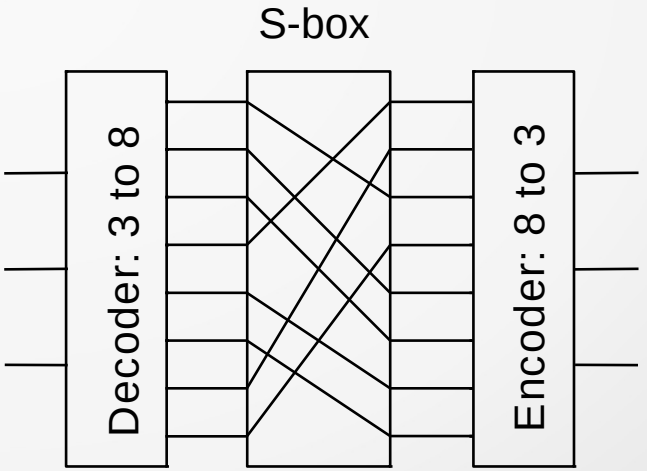
- Gli algoritmi crittografici moderni si dividono in due grandi famiglie
  - **Algoritmi a chiave segreta o simmetrici:** la chiave è segreta e l'algoritmo è composto da una complicata serie di sostituzioni e trasposizioni
  - **Algoritmi a chiave pubblica o asimmetrici:** le chiavi sono due, una pubblica e una privata e si basano sull'aritmetica modulare o sui logaritmi discreti

Algoritmi a chiave segreta

- Utilizzo di un algoritmo molto complesso tramite concatenazione di blocchi di trasposizione e sostituzione



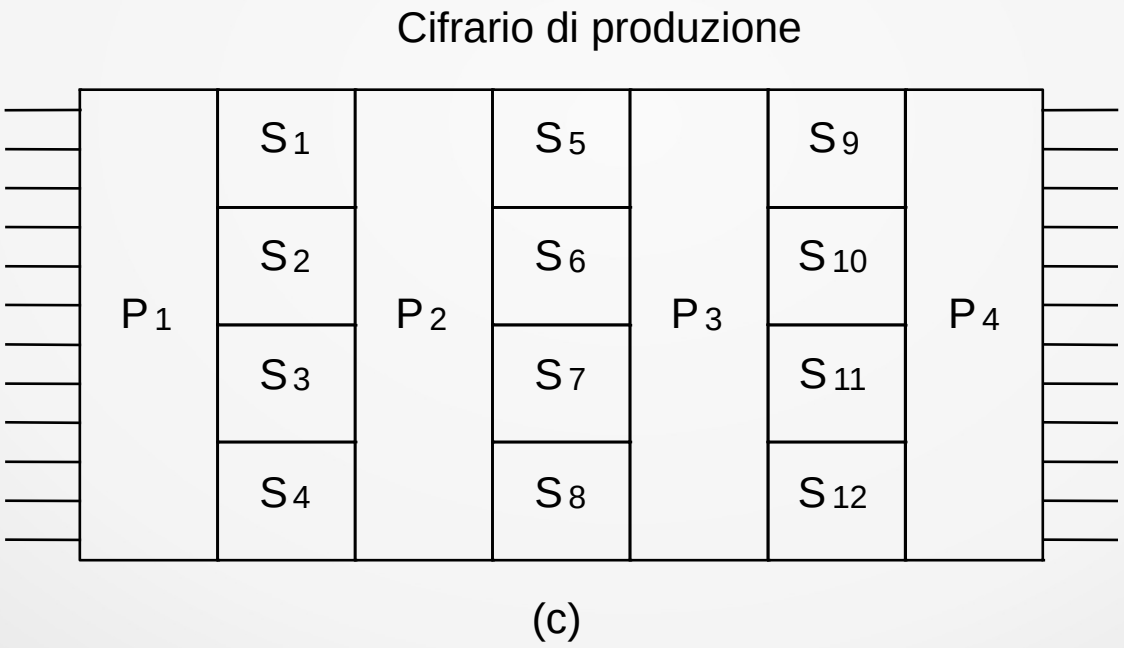
Blocco di trasposizione



Blocco di sostituzione

Algortimi a chiave segreta

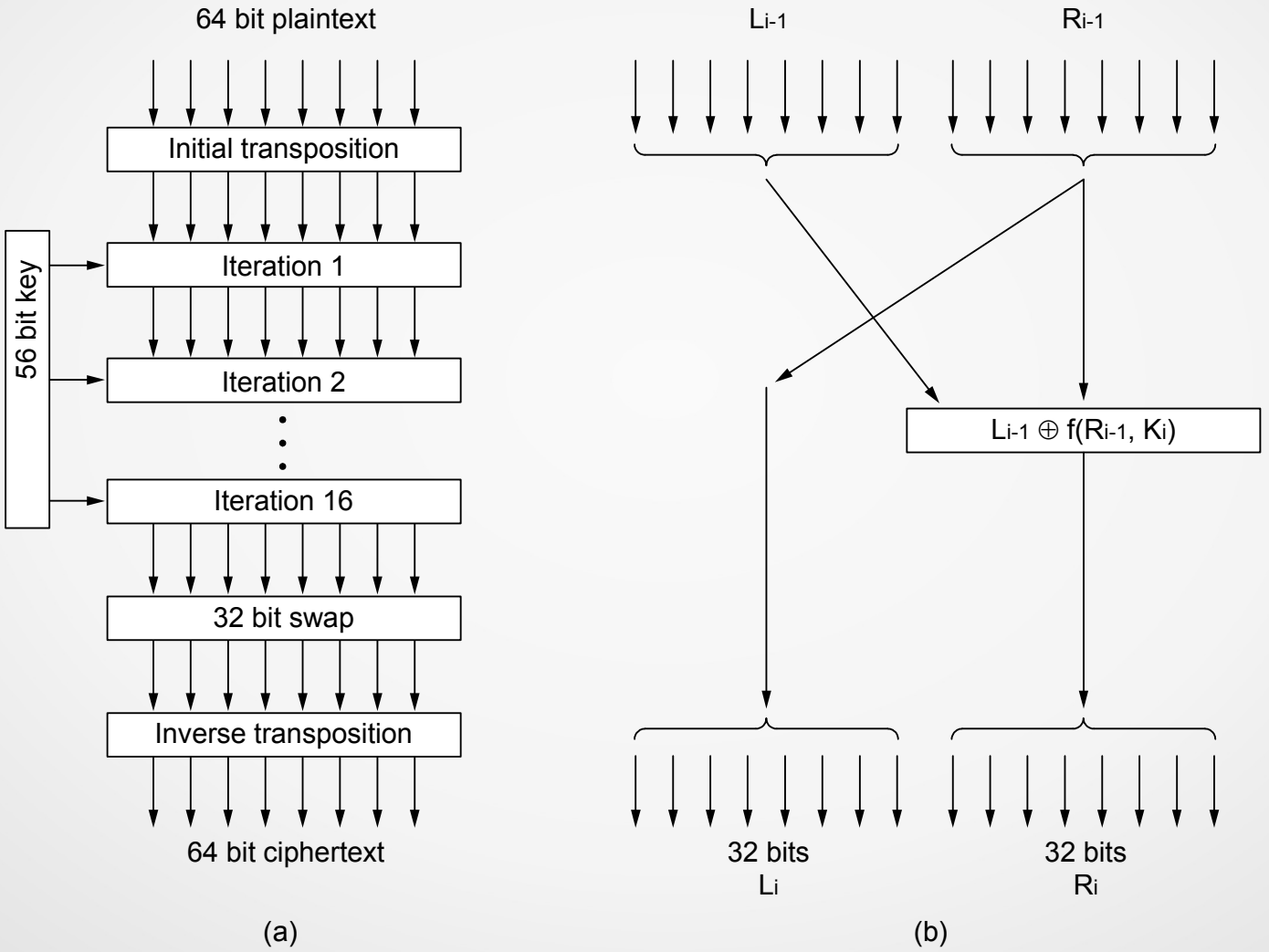
- Concatenazione di più blocchi per la creazione di un cifrario



DES - Data Encryption Standard

- Sviluppato da IBM nel 1977 e adottato come standard ufficiale dal governo statunitense per le informazioni non classificate
- Blocchi di 64 bit di testo in chiaro generano 64 bit di testo cifrato
- L'algoritmo è parametrizzato da una chiave a 56 bit.

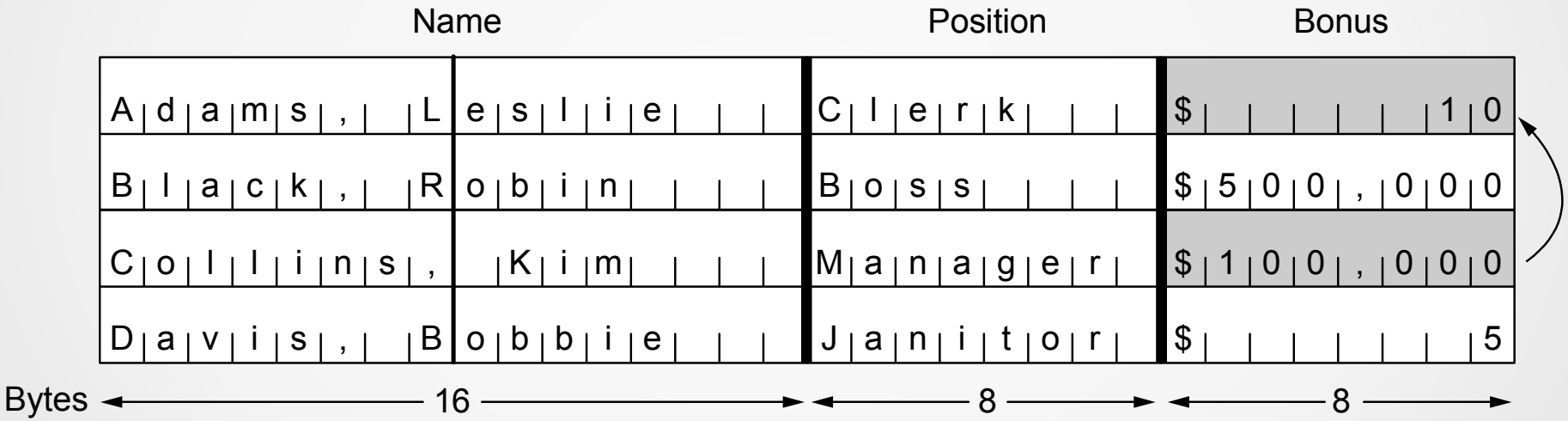
DES - Data Encryption Standard



DES: problemi e varianti

- Al di là della sua complessità il DES è un cifrario a sostituzione monoalfabetico con caratteri di lunghezza 64 bit
- Anche se decoficare il codice può essere difficile, esistono situazioni in cui è molto facile cambiare il testo codificato per ottenerne una versione alterata ma valida

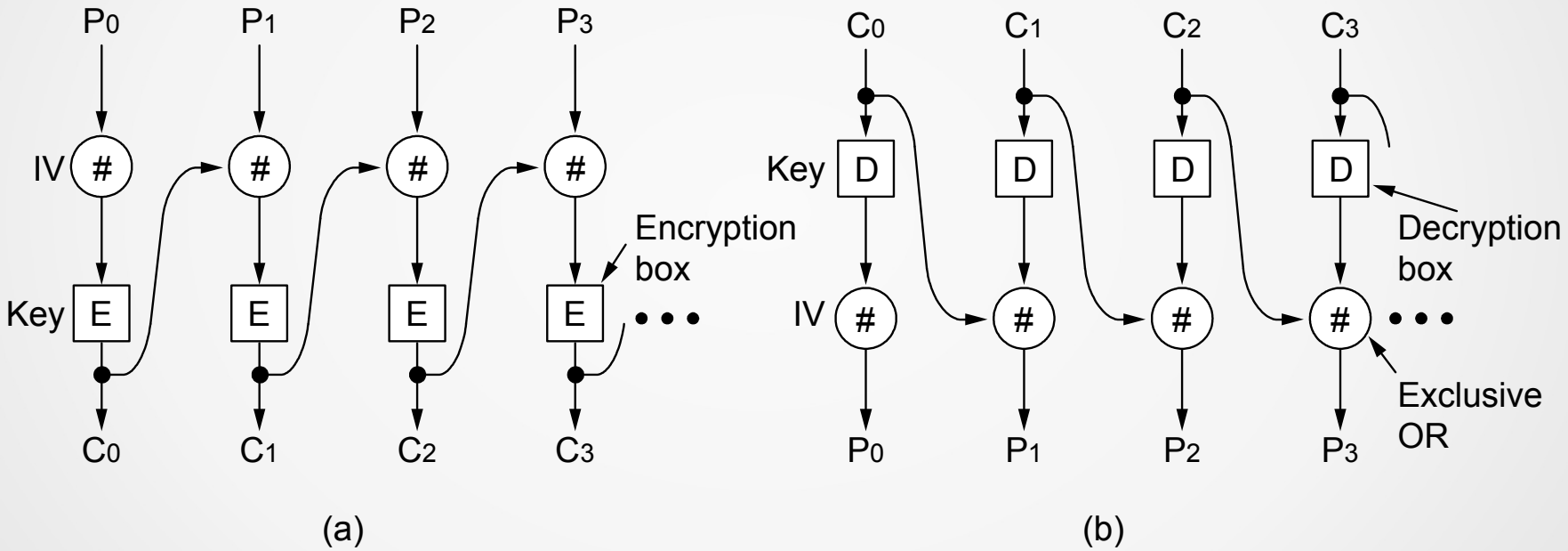
DES - Problemi e varianti



DES: problemi e varianti

- Per prevenire questo tipo di attacchi si concatenano i blocchi del DES in modo che eventuali scambi portino ad ottenere messaggi non validi
- Modalità:
  - concatenazione a blocchi
  - feedback
  - output feedback

DES - Concatenazione a blocchi



DES - Rottura del codice

- Con chiavi lunghe 56 bit 2^{56} chiavi (inizialmente chiave a 112 bit)
- Esistono progetti per macchine in grado di rompere DES in meno di quattro ore, però molto costose
- Altra idea: la Lotteria Cinese

DES - La Lotteria Cinese

- Idea:
  - Fornire ogni radio/televisione di un processore DES in grado di effettuare 1.000.000 codifiche/s ognuno con uno spazio delle chiavi differente
  - Mandare in broadcast la coppia testo in chiaro/ testo cifrato
  - Con 1.200.000.000 apparecchi in 60 s verrebbe esplorato tutto lo spazio delle chiavi
  - Messaggio di vincita della lotteria

DES – Attacchi reali

- EFF DES Cracker: costo circa 250000 dollari (1998), attacco a forza bruta con successo in circa 2 giorni.
- COPACABANA machine: costo circa 10000 dollari (2006) utilizzando hardware commerciale, attacco a forza bruta con successo in circa una settimana

DES: miglioramenti

- Applicandolo due volte con due chiavi diverse si ottengono 2^{112} chiavi (circa 5×10^{33})
- Impossibilità di esplorare tutto lo spazio delle chiavi
- In realtà esiste un attacco (meet-in-the-middle) che riduce lo spazio delle chiavi a 2^{57}
- Stessa difficoltà del DES semplice

Attacco Meet-in-the-middle

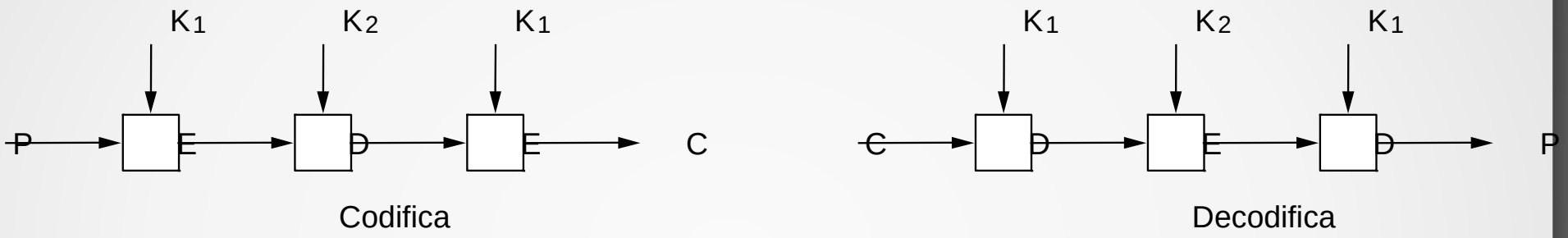
- Conoscendo un testo in chiaro P e il testo cifrato corrispondente C

$$C=E_{K1}(E_{K2}(P))$$

- Trovo tutte le codifiche di P usando tutte le chiavi possibili (2^{56})
- Trovo tutte le decodifiche di C usando tutte le chiavi possibili (2^{56})
- Cerco una corrispondenza poiché

$$D_{K1}(C)= E_{K2}(P)$$

DES - Codifica tripla



- EDE al posto di EEE per motivi di retrocompatibilità (basta porre $K_1=K_2$)
- Non si conoscono metodi per forzarlo

AES – Advanced Encryption Standard

- Sostituto del DES adottato dal governo statunitense per informazioni classificate Top Secret
- Chiave a 128, 192 o 256 bit
- Blocchi da 128 bit

Un'anticipazione golosa

- Due volontari:
- Prendete i numeri 753 e 413
- Scegliete un numero a caso ***x*** (e ricordatevelo) minore di 413
- Elevate 753 alla ***x*** e fate modulo 413
- Dite a voce alta il numero ottenuto, chiamiamolo ***y***
- Prendete ***y*** e elevatelo a ***x*** modulo 413