Crittografia
e algoritmi genetici

I

Basi di crittografia per testi

Crittografia

- La crittografia si occupa di come nascondere il significato di un messaggio T a chiunque non sia il destinatario
- Tramite la scelta di un algoritmo C e di una chiave k, il messaggio viene criptato dal mittente in modo da non renderne comprensibile il contenuto
- Il destinatario, a cui sono noti chiave e algoritmo, può decrittare il messaggio e ottenere il testo in chiaro

Crittografia

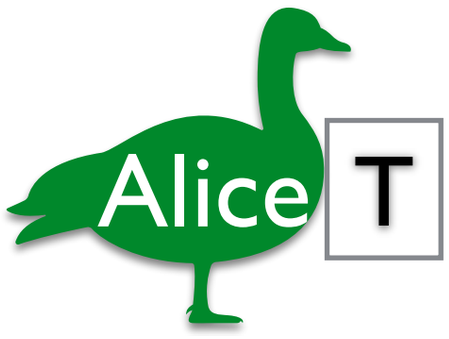
- La crittografia si occupa di come nascondere il significato di un messaggio T a chiunque non sia il destinatario
- Tramite la scelta di un algoritmo C e di una chiave k, il messaggio viene criptato dal mittente in modo da non renderne comprensibile il contenuto
- Il destinatario, a cui sono noti chiave e algoritmo, può decrittare il messaggio e ottenere il testo in chiaro

Crittografia

- La crittografia si occupa di come nascondere il significato di un messaggio T a chiunque non sia il destinatario
- Tramite la scelta di un algoritmo C e di una chiave k, il messaggio viene criptato dal mittente in modo da non renderne comprensibile il contenuto
- Il destinatario, a cui sono noti chiave e algoritmo, può decrittare il messaggio e ottenere il testo in chiaro

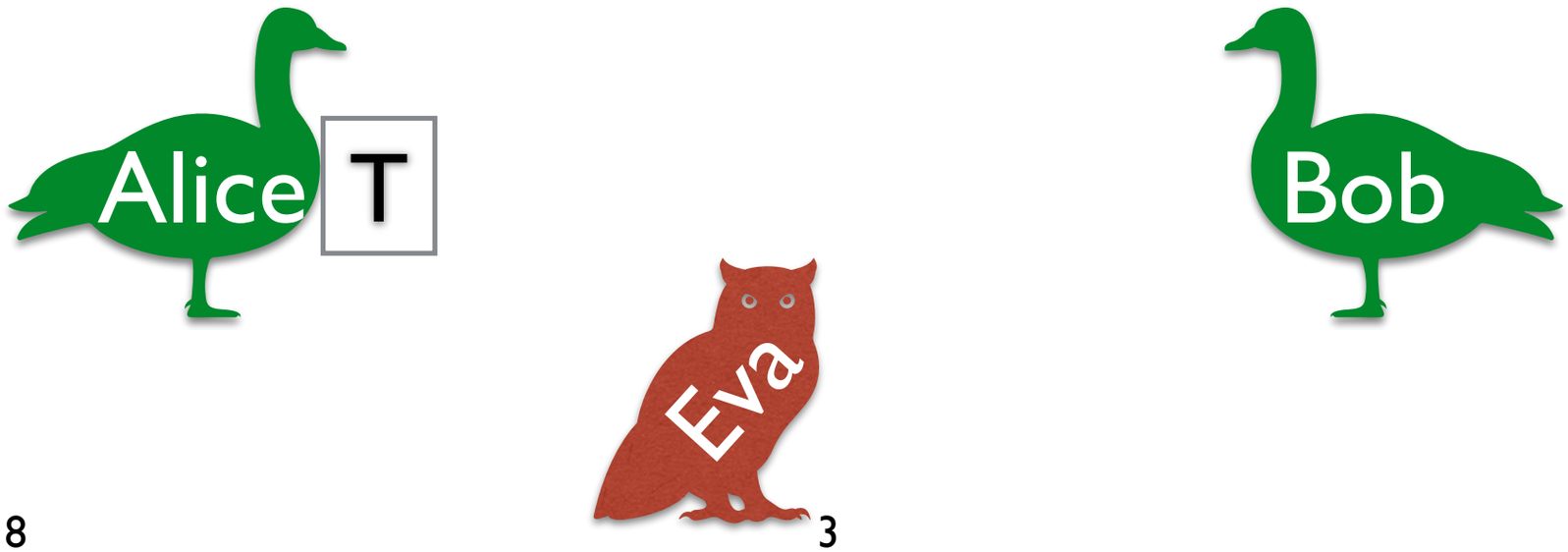
Crittografia

- La crittografia si occupa di come nascondere il significato di un messaggio T a chiunque non sia il destinatario
- Tramite la scelta di un algoritmo C e di una chiave k, il messaggio viene criptato dal mittente in modo da non renderne comprensibile il contenuto
- Il destinatario, a cui sono noti chiave e algoritmo, può decrittare il messaggio e ottenere il testo in chiaro



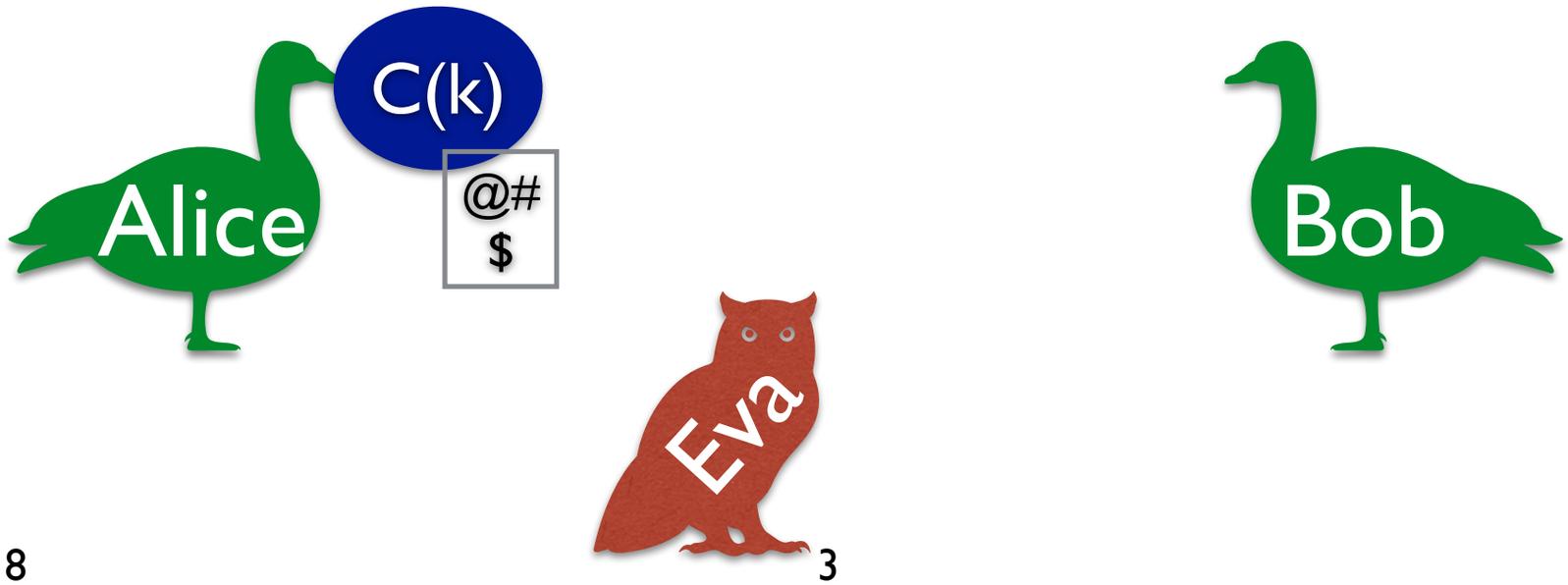
Crittografia

- La crittografia si occupa di come nascondere il significato di un messaggio T a chiunque non sia il destinatario
- Tramite la scelta di un algoritmo C e di una chiave k, il messaggio viene criptato dal mittente in modo da non renderne comprensibile il contenuto
- Il destinatario, a cui sono noti chiave e algoritmo, può decrittare il messaggio e ottenere il testo in chiaro



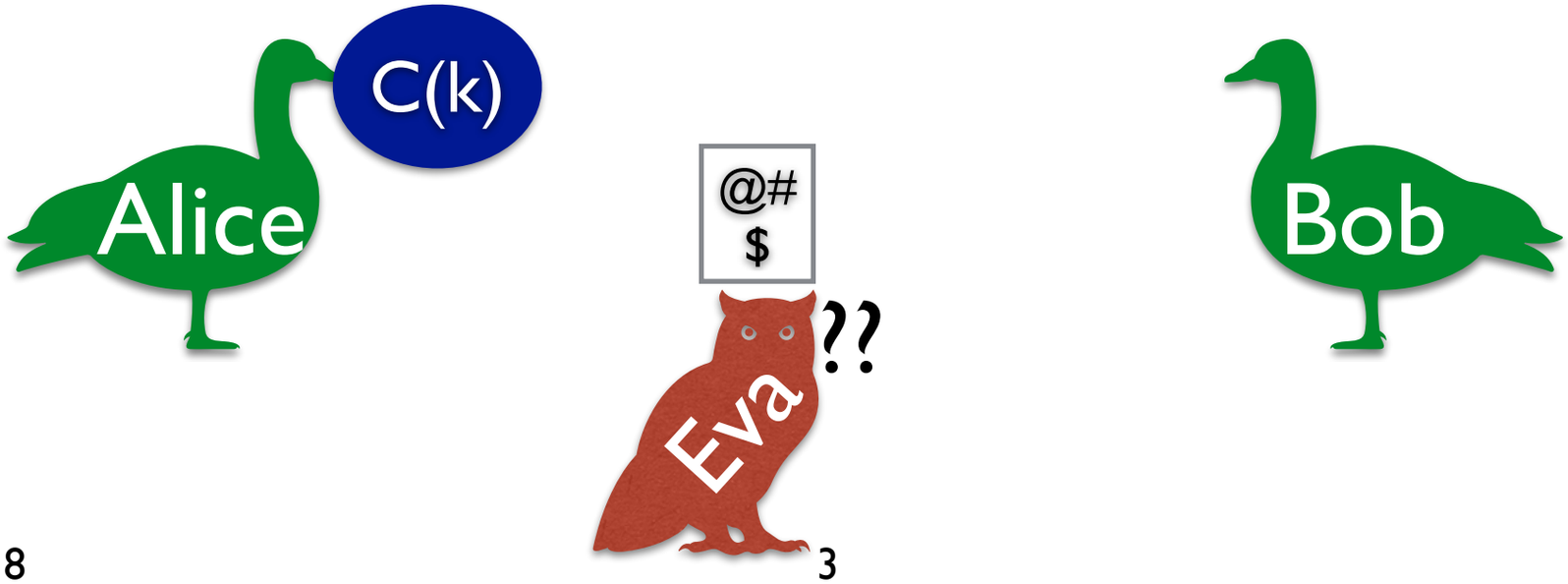
Crittografia

- La crittografia si occupa di come nascondere il significato di un messaggio T a chiunque non sia il destinatario
- Tramite la scelta di un algoritmo C e di una chiave k, il messaggio viene criptato dal mittente in modo da non renderne comprensibile il contenuto
- Il destinatario, a cui sono noti chiave e algoritmo, può decrittare il messaggio e ottenere il testo in chiaro



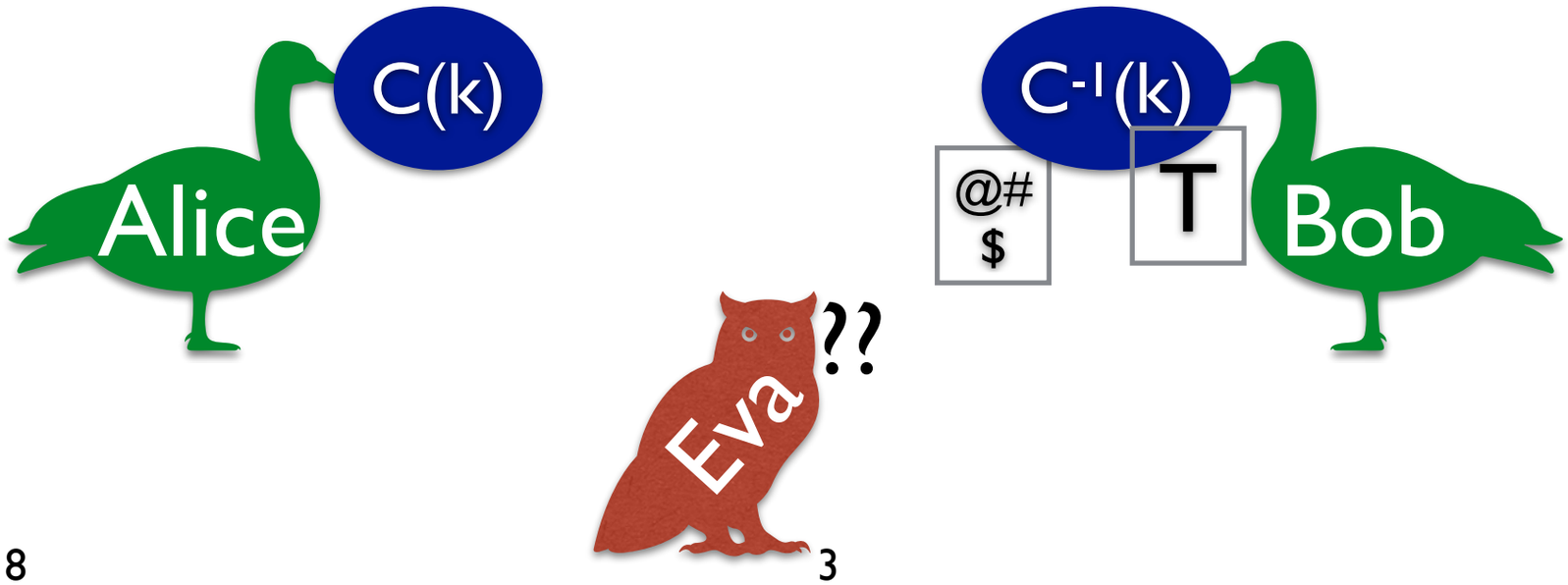
Crittografia

- La crittografia si occupa di come nascondere il significato di un messaggio T a chiunque non sia il destinatario
- Tramite la scelta di un algoritmo C e di una chiave k, il messaggio viene criptato dal mittente in modo da non renderne comprensibile il contenuto
- Il destinatario, a cui sono noti chiave e algoritmo, può decrittare il messaggio e ottenere il testo in chiaro



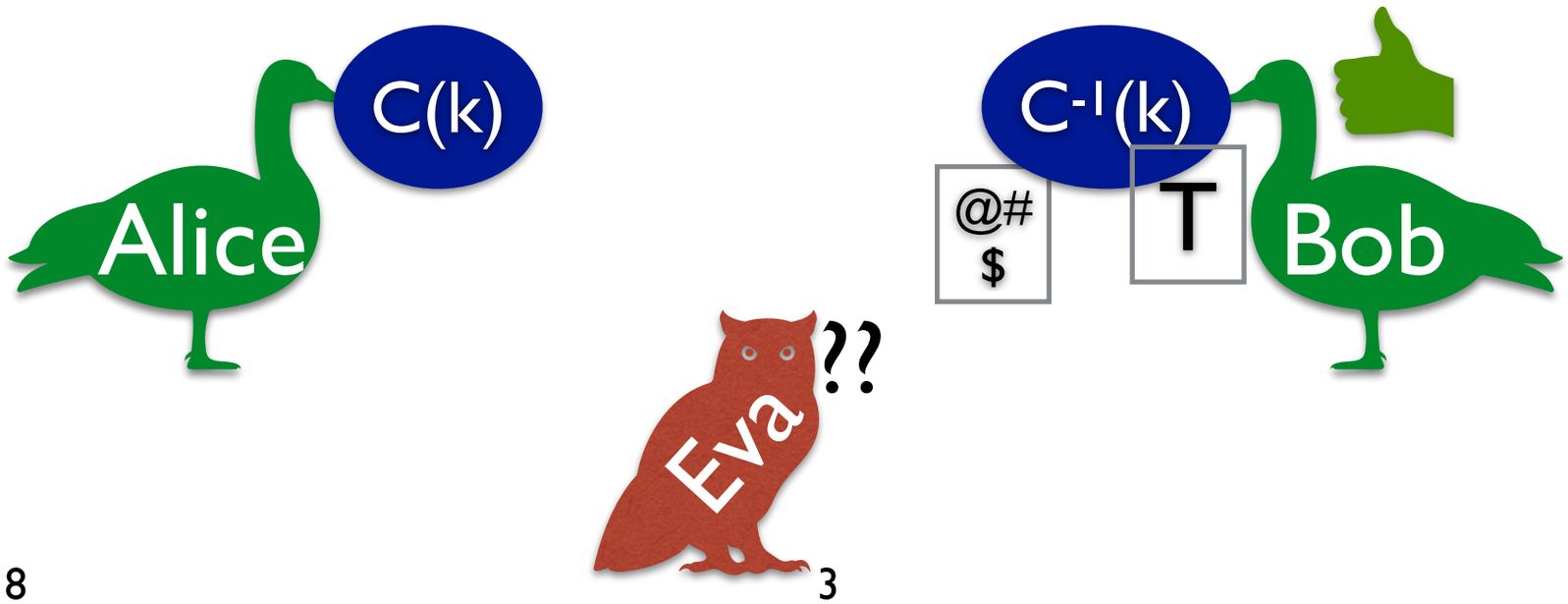
Crittografia

- La crittografia si occupa di come nascondere il significato di un messaggio T a chiunque non sia il destinatario
- Tramite la scelta di un algoritmo C e di una chiave k, il messaggio viene criptato dal mittente in modo da non renderne comprensibile il contenuto
- Il destinatario, a cui sono noti chiave e algoritmo, può decrittare il messaggio e ottenere il testo in chiaro



Crittografia

- La crittografia si occupa di come nascondere il significato di un messaggio T a chiunque non sia il destinatario
- Tramite la scelta di un algoritmo C e di una chiave k, il messaggio viene criptato dal mittente in modo da non renderne comprensibile il contenuto
- Il destinatario, a cui sono noti chiave e algoritmo, può decrittare il messaggio e ottenere il testo in chiaro



Crittografia mono-alfabetica (1)

- A ogni lettera corrisponde una e una sola altra lettera
  - Caso più semplice: cifratura di Cesare. Ogni lettera viene spostata di n posizioni in avanti nell'alfabeto
  - Ad esempio, prendiamo come chiave n=3:
    `ciao io mi chiamo marco` Testo in chiaro
    `fldr lr pl fkldpr pdufr` Testo crittato
  - Abbiamo N=26 soluzioni (le lettere dell'alfabeto)

Crittografia mono-alfabetica (2)

- A ogni lettera corrisponde una e una sola altra lettera
  - Caso più complesso: si mappa l'alfabeto in una permutazione:

    `abcdefghijklmnopqrstuvwxyz`
    `zysbengapjciqlwdxhvroukmtf`
  - Ad esempio:

    `ciao io mi chiamo marco`
    `spzw pw qp sapzqw qzhsw`
  - Ho 26!~4x10^{26} soluzioni
  - Di solito i metodi mono-alfabetici sono poco sicuri: possono essere decodificati con un'analisi della frequenza delle lettere

Crittografia poli-alfabetica

- A una stessa lettera possono corrispondere diverse lettere
  - Esempio: cifrario di Vigenère. La chiave è una parola.
    La codifica avviene sommando la posizione nell'alfabeto di ogni lettera del testo con quella corrispondente della chiave:
    `ciaoiomichiamomarco` Testo in chiaro
    `pippopippopipppopipp` chiave (ripetuta)
    `srqexevyswyjcebqase` Testo crittato
  - Ho $N=26^L$ possibili soluzioni, dove L è la lunghezza della chiave
  - Se L > lunghezza messaggio, il messaggio è decrittabile solo conoscendo la chiave

Compito per oggi

- Scrivere un modulo python che codifichi e decodifichi messaggi usando i 3 metodi presentati
- Il carattere spazio può essere o meno parte dell'alfabeto
- NB: le stringhe sono immutabili

```
> a = "ciao"
 > a[2] == "a"
True
> a[2] = "b"
TypeError: 'str' object does not support item
assignment
> b = list(a)
> b[2] = "b"
> print "".join(b)
cibo
```