Honey Encryption

per messaggi in Linguaggio Naturale

Relatore
Prof. Luca Giuzzi

Laureando
Yanez Diego Parolin

Tesi di Laurea Triennale – Ingegneria Informatica – 11 settembre 2019

Honey Encryption

(A.Juel – Eurocrypt 2014)

“Produces a ciphertext, which, when decrypted with an incorrect key as guessed by the attacker, presents a plausible-looking yet incorrect plaintext password or encryption key.”[1]

Michael Mimoso

Honey Encryption

(A.Juel – Eurocrypt 2014)

"Produces a ciphertext, which, when decrypted with an incorrect key as guessed by the attacker, presents a plausible-looking yet incorrect plaintext password or encryption key."[1]

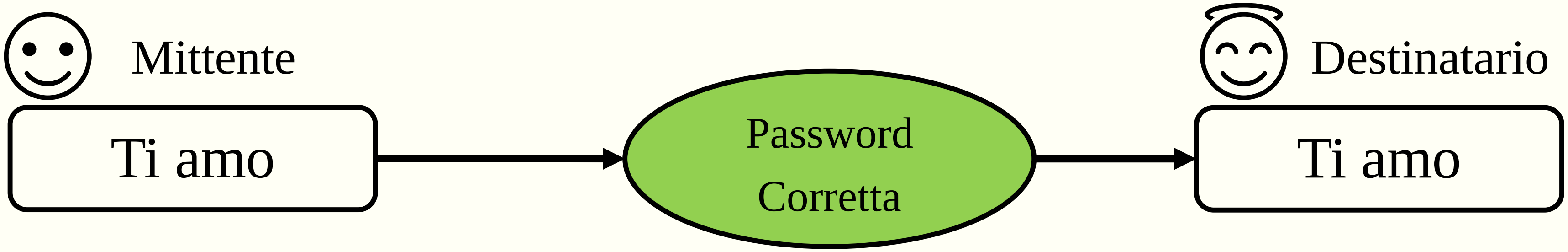
Michael Mimoso

OBIETTIVO → **EVITARE BRUTE FORCE ATTACK**

Honey Encryption – Concetto

Decrittazione con password errata

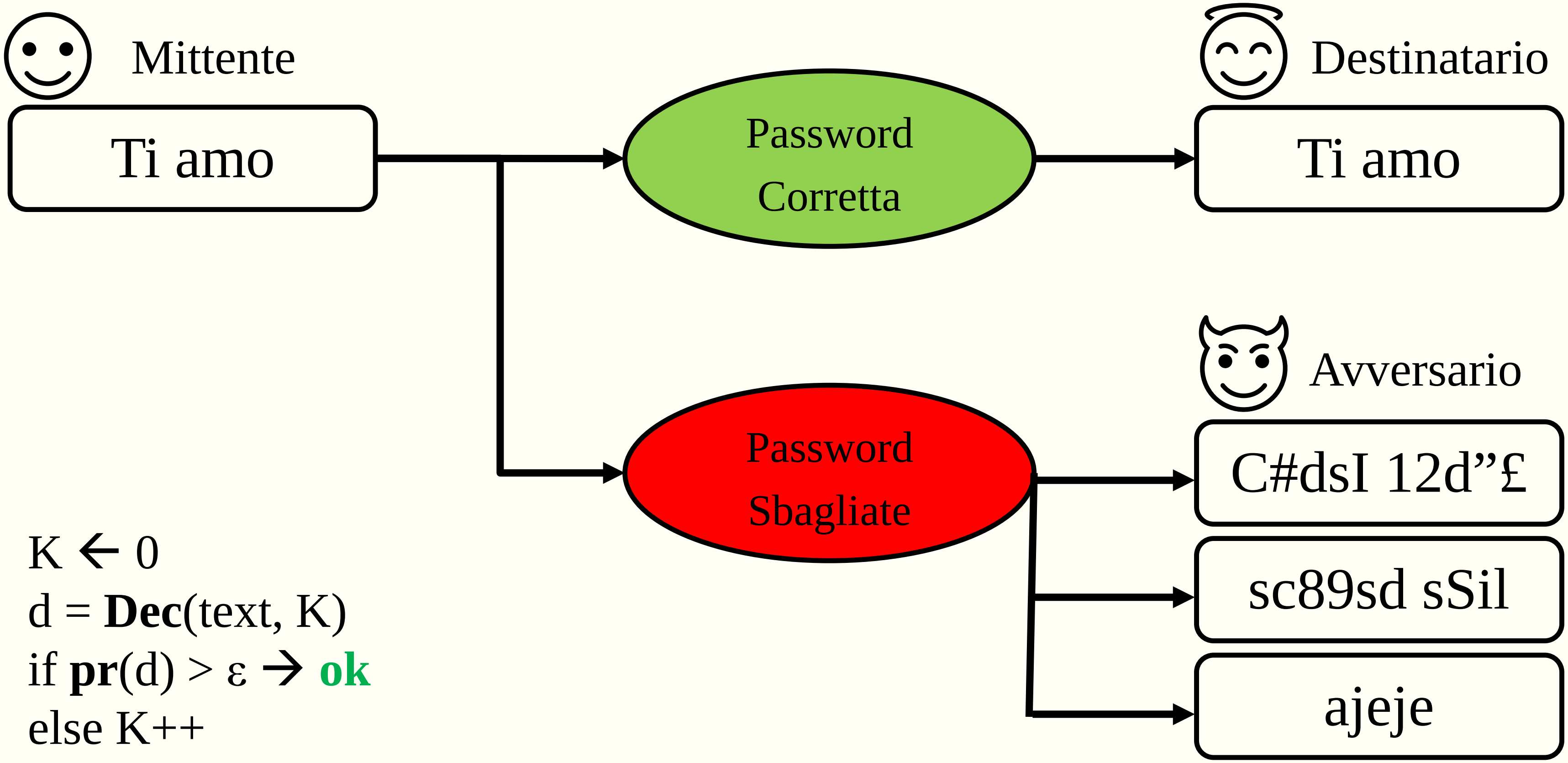
Sistema Crittografico Generico



Honey Encryption – Concetto

Decrittazione con password errata

Sistema Crittografico Generico

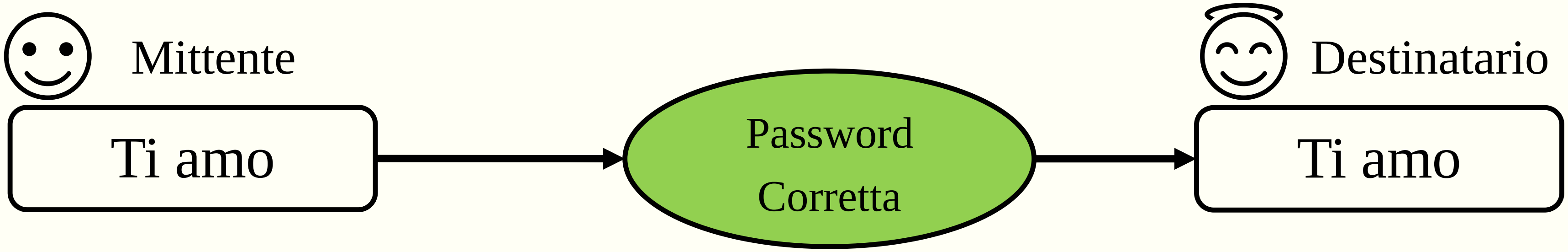


```
K ← 0
d = Dec(text, K)
if pr(d) > ε → ok
else K++
```

Honey Encryption – Concetto

Decrittazione con password errata

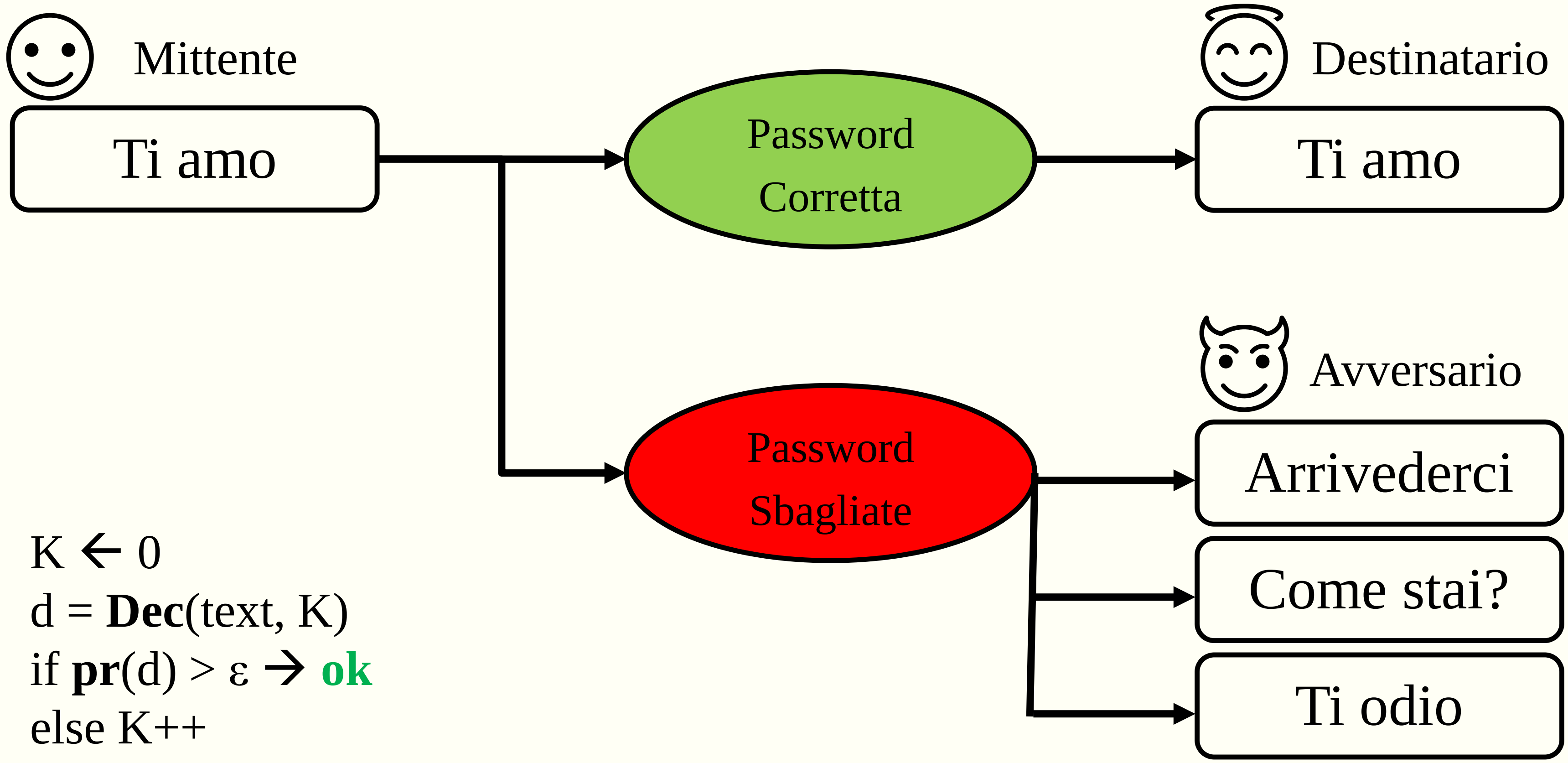
HONEY ENCRYPTION



Honey Encryption – Concetto

Decrittazione con password errata

HONEY ENCRYPTION



```
$K \leftarrow 0$
$d = \mathbf{Dec}(text, K)$
if $\mathbf{pr}(d) > \varepsilon \rightarrow$ ok
else K++
```

Honey Encryption – Struttura e Funzionamento

- ❖ Message Space $\mathcal{M}$
- ❖ Seed Space **S**
- ❖ DTE Distribution Transforming Encoder
  - Mappa $\mathcal{M}$ su **S** attraverso apposite funzioni
  - Decodifica e Codifica seed e messaggi

Honey Encryption – Struttura e Funzionamento

- Message Space $\mathcal{M}$
- Seed Space $\mathbf{S}$
- DTE Distribution Transforming Encoder
  - Mappa $\mathcal{M}$ su $\mathbf{S}$ attraverso apposite funzioni
  - Decodifica e Codifica seed e messaggi

$\mathcal{M}$

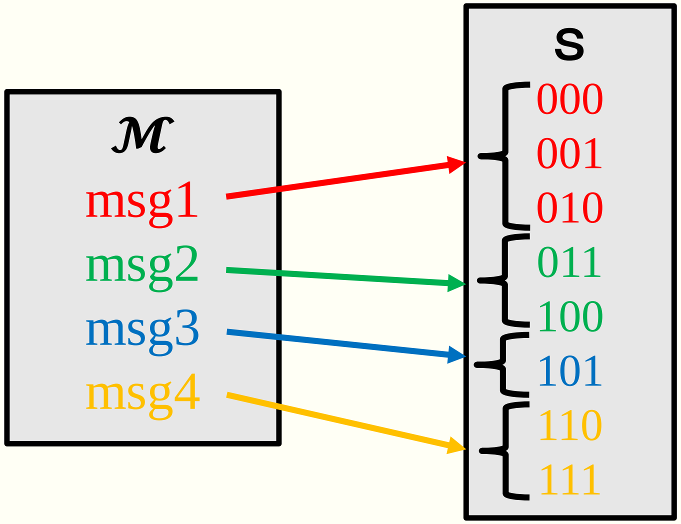
msg1
msg2
msg3
msg4

$\mathbf{S}$

000
001
010
011
100
101
110
111

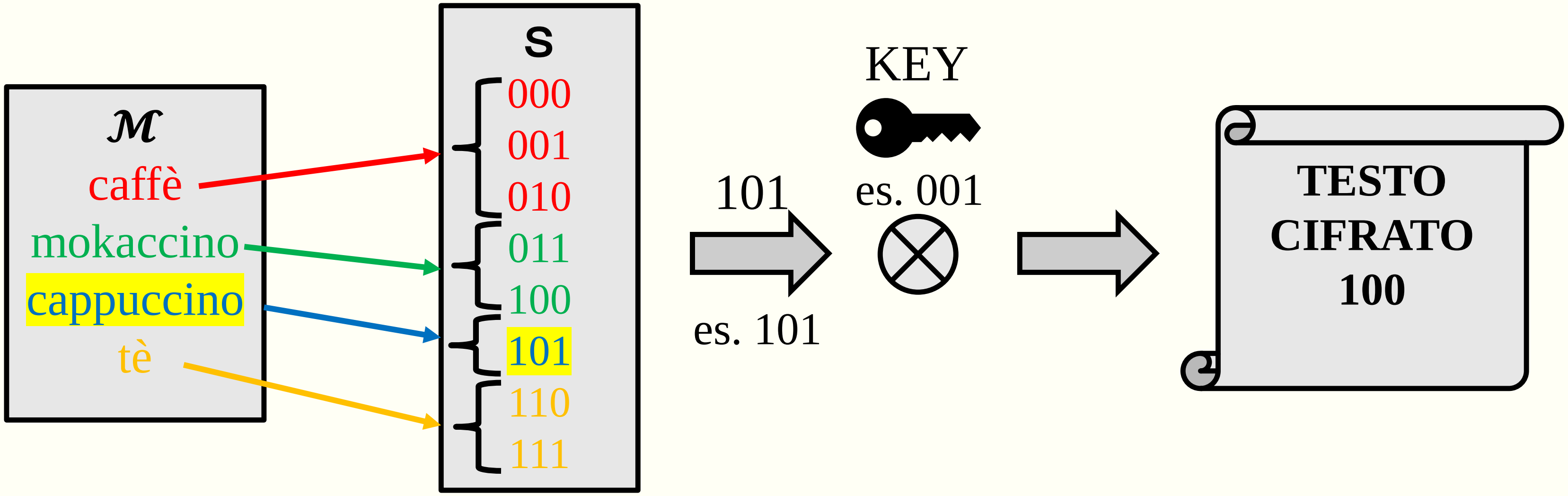
Honey Encryption – Struttura e Funzionamento

- Message Space $\mathcal{M}$
- Seed Space **S**
- DTE Distribution Transforming Encoder
  - Mappa $\mathcal{M}$ su **S** attraverso apposite funzioni
  - Decodifica e Codifica seed e messaggi



Honey Encryption – Struttura e Funzionamento

- Message Space $\mathcal{M}$
- Seed Space **S**
- DTE Distribution Transforming Encoder
    - Mappa $\mathcal{M}$ su **S** attraverso apposite funzioni
    - Decodifica e Codifica seed e messaggi



Honey Encryption - Implementazioni

DATI STRUTTURATI	
Esistenza di REGOLE logico-matematice precise per la generazione del $\mathcal{M}$ ▪ **Carte di Credito** Honey Encryption for Credit Card Number – MIT [2] ▪ **IID** Protecting Private Data by Honey Encryption – Hindawi [3] ▪ **FILE** Implementing the Honey Encryption for Securing Public Cloud Data Storage – USM [4]	

Honey Encryption - Implementazioni

DATI STRUTTURATI	**DATI FLESSIBILI (Linguaggio Naturale)**
Esistenza di algoritmi per la generazione del $\mathcal{M}$ ▪ **Carte di Credito** Honey Encryption for Credit Card Number – MIT [2] ▪ **IID** Protecting Private Data by Honey Encryption – Hindawi [3] ▪ **FILE** Implementing the Honey Encryption for Securing Public Cloud Data Storage – USM [4]	*Dati dinamici, la cui struttura non è regolata da regole univoche e dettagliate* ▪ **Linguaggio Naturale** Honey Chatting – CIST [5] Novel Approach for the Adaptation of Honey Encryption to Support Natural Language Message – USM [6] ☹

Il mio progetto – Strumenti utilizzati

Honey Encryption

Per messaggi in Linguaggio Naturale

- **Python** – Linguaggio di Programmazione
- **SpaCy**[7]– Parser Linguaggio Naturale
  Semplificato e ottimizzato per Python rispetto allo Stanford Parser[8]
- **Pattern** [9] + **Inflect** [10] – Engine NLP Python
  Declinazione e coniugazione dei lemmi

Il mio progetto – Strumenti utilizzati

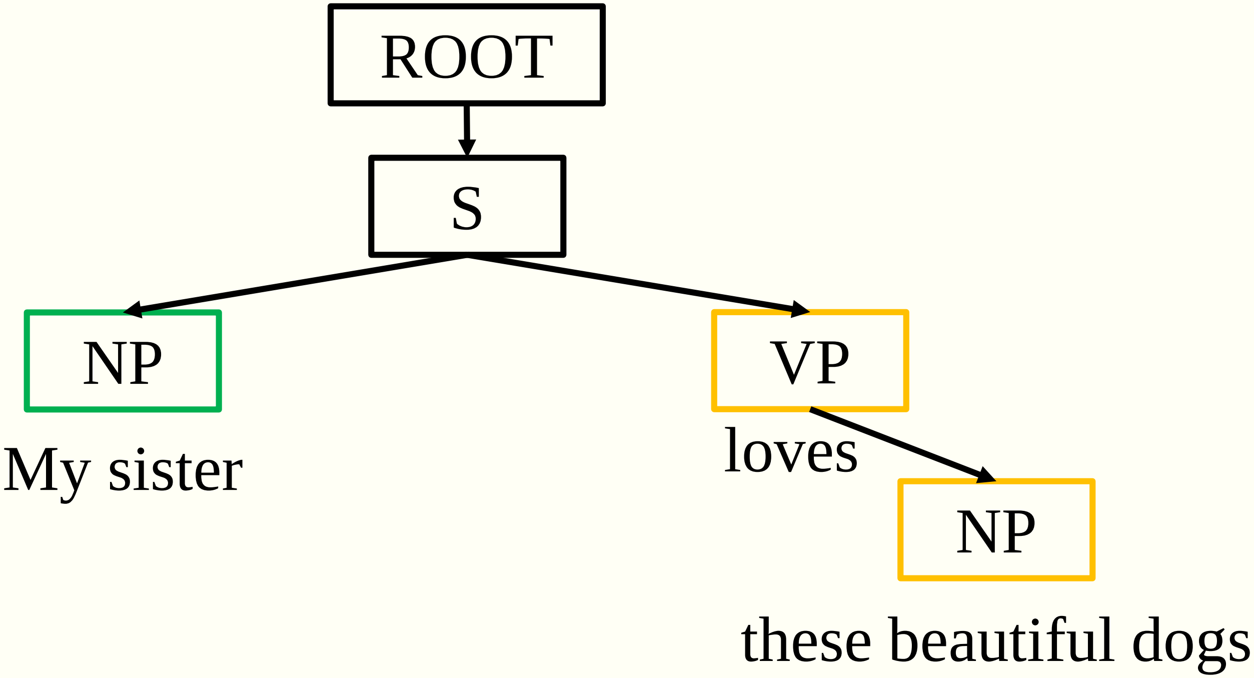
Honey Encryption

Per messaggi in Linguaggio Naturale

- **Python** – Linguaggio di Programmazione
- **SpaCy**[7]– Parser Linguaggio Naturale
  Semplificato e ottimizzato per Python rispetto allo Stanford Parser[8]
- **Pattern** [9] **+ Inflect** [10] – Engine NLP Python
  Declinazione e coniugazione dei lemmi
- **Dizionari in locale** – Storage dei dati
  Per la struttura della frase per i verbi, aggettivi, nomi ecc.
- **AES + PBKDF2** – Crittografia

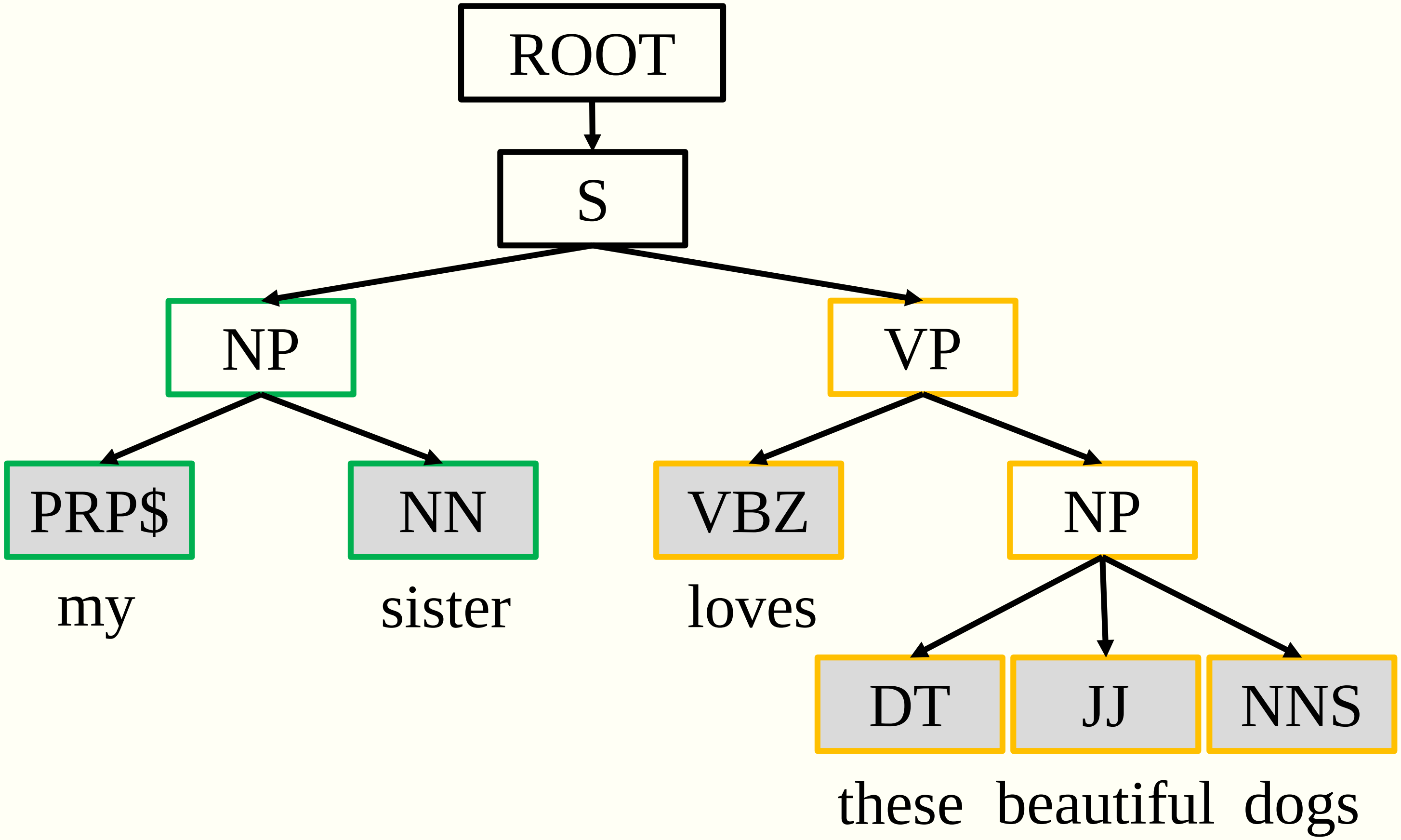
Il mio progetto - PARSER

“My sister loves these beautiful dogs”

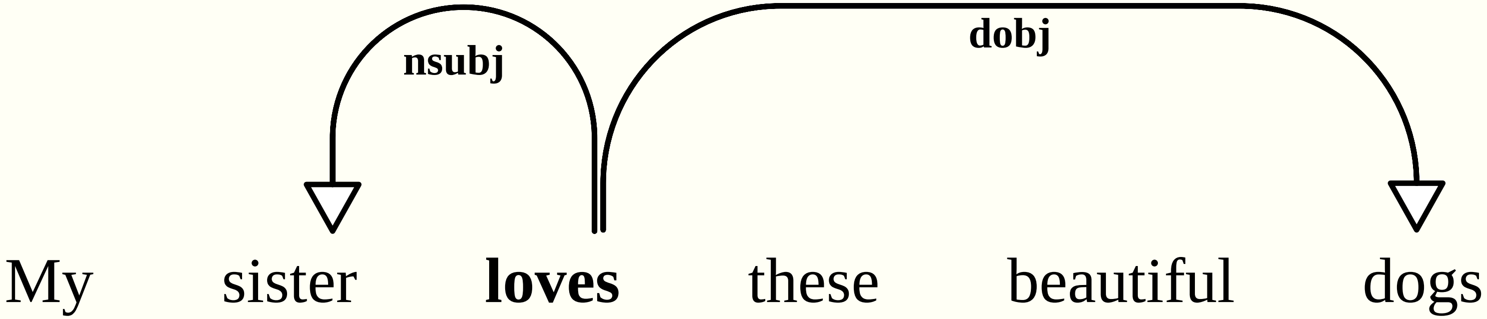


Il mio progetto - PARSER

“My sister loves these beautiful dogs”

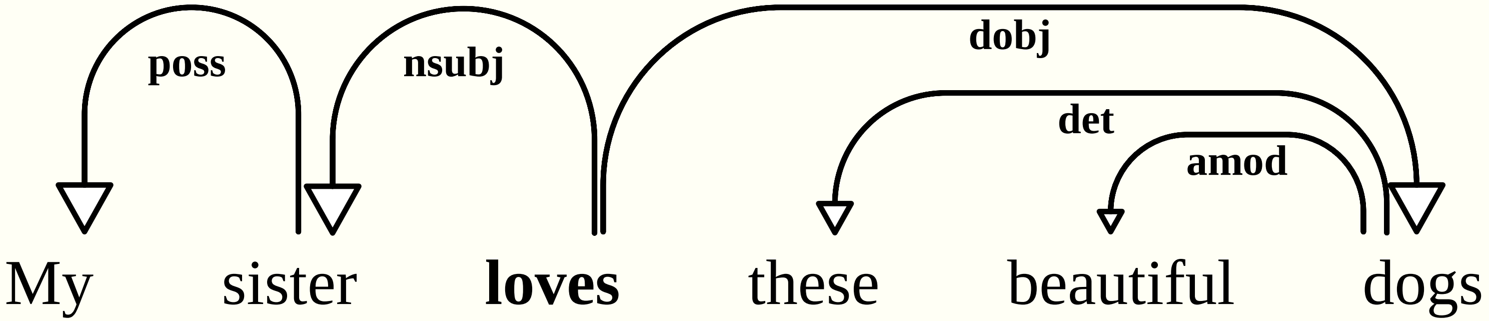


Il mio progetto - PARSER



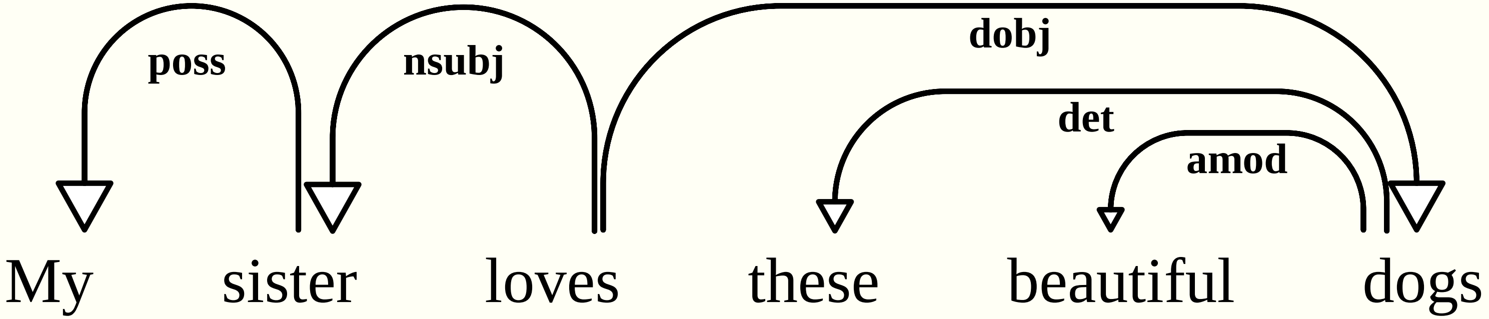
My sister **loves** these beautiful dogs

Il mio progetto - PARSER



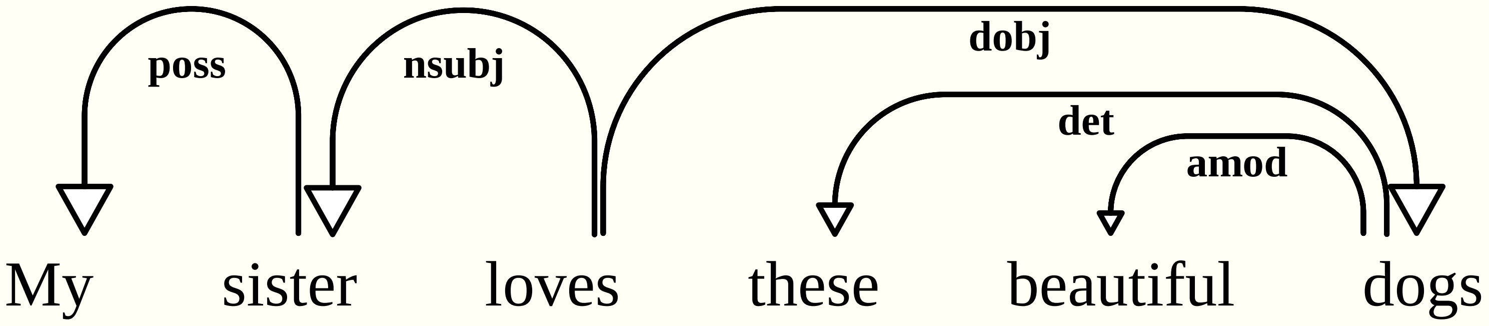
UNIVERSITÀ DEGLI STUDI DI BRESCIA

Il mio progetto - PARSER



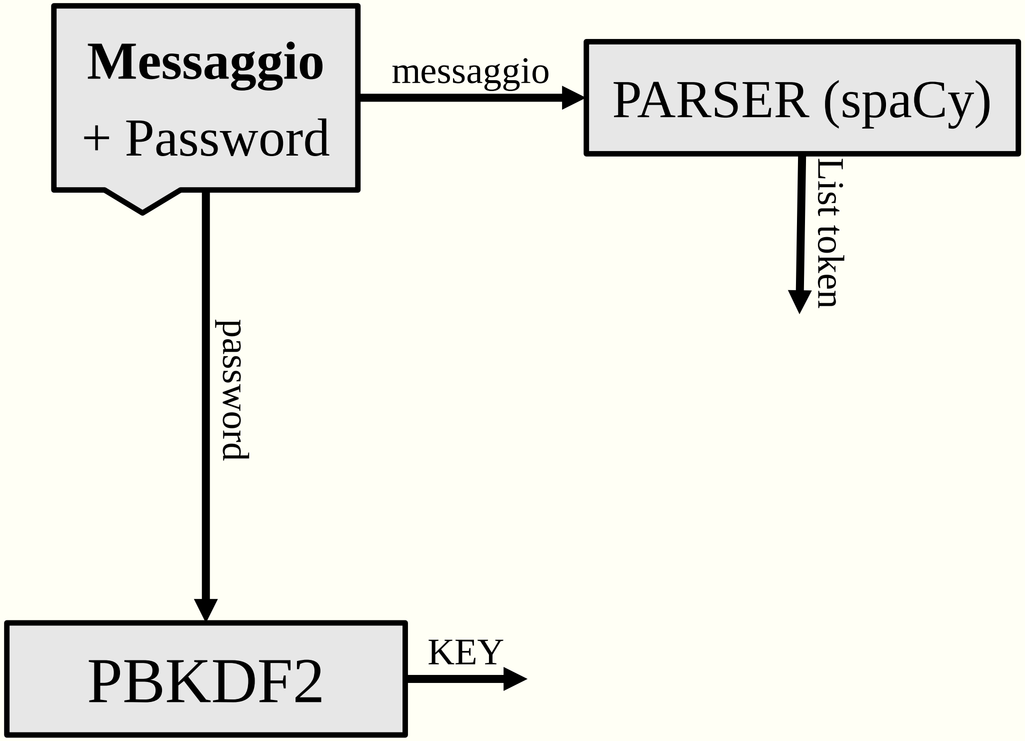
Text	lemma	Index	POS	POS TAG	DEP	P_index
My	my	***0***	DET	***PRP$***	***poss***	***1***
sister	sister	***1***	NOUN	***NN***	***nsubj***	***2***
loves	love	***2***	VERB	***VBZ***	***ROOT***	***2***
these	these	***3***	DET	***DT***	***det***	***5***
beautiful	beautiful	***4***	ADJ	***JJ***	***amod***	***5***
dogs	dog	***5***	NOUN	***NNS***	***dobj***	***2***

Il mio progetto - PARSER

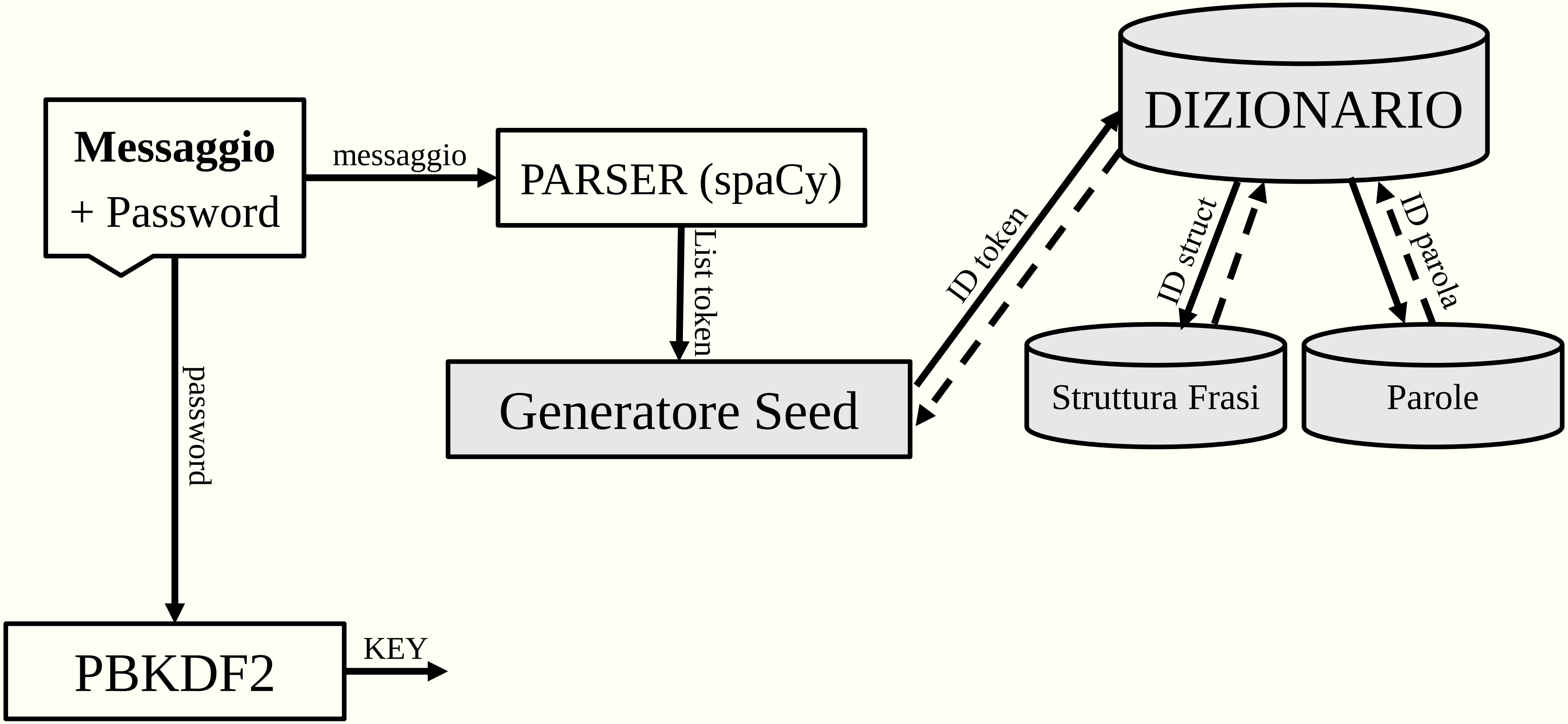


Text	lemma	Index	POS	POS TAG	DEP	P_index
My	my	***0***	DET	***PRP$***	***poss***	***1***
sister	sister	***1***	NOUN	***NN***	***nsubj***	***2***
loves	love	***2***	VERB	***VBZ***	***ROOT***	***2***
these	these	***3***	DET	***DT***	***det***	***5***
beautiful	beautiful	***4***	ADJ	***JJ***	***amod***	***5***
dogs	dog	***5***	NOUN	***NNS***	***dobj***	***2***

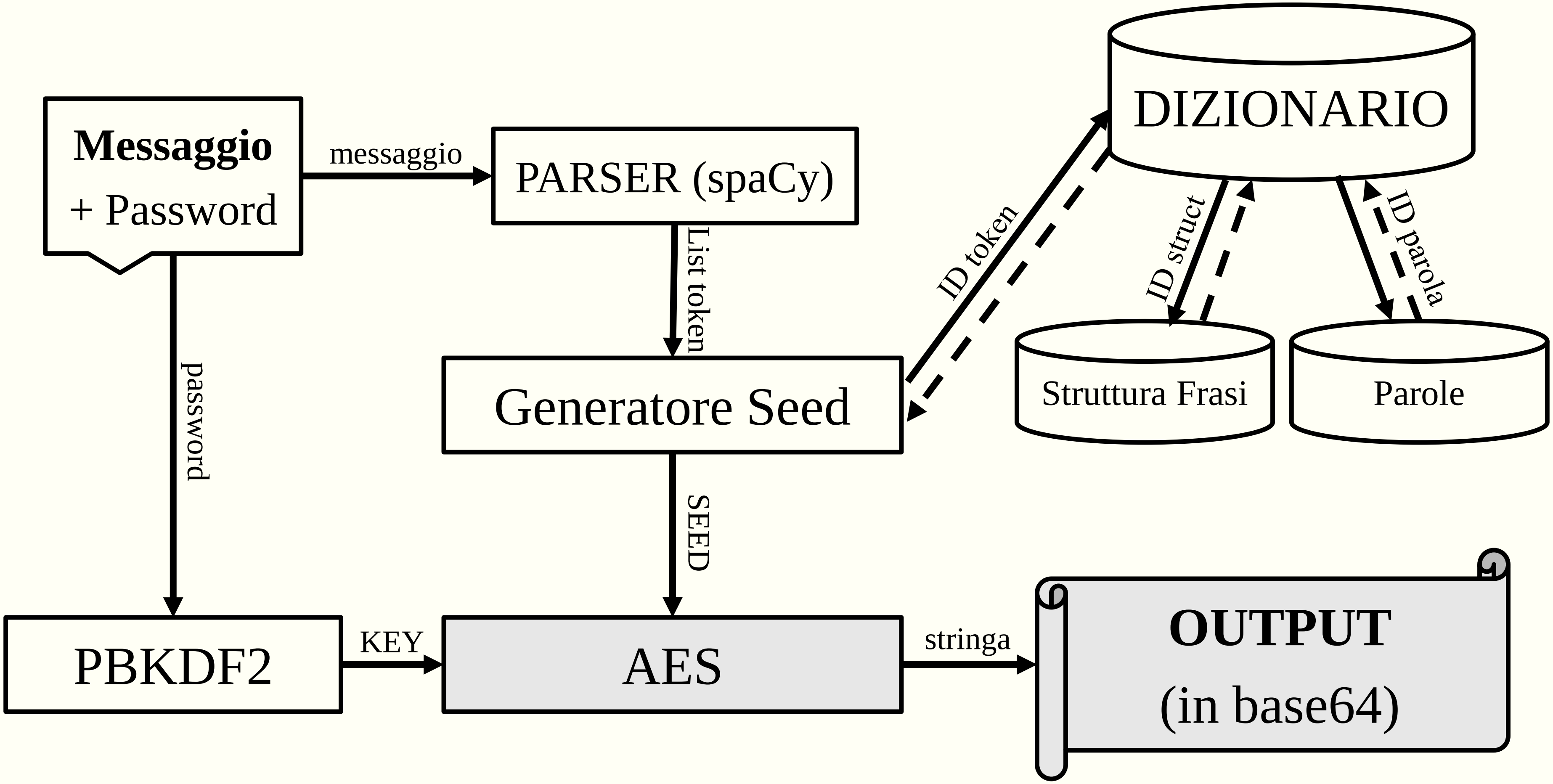
Il mio progetto – Schema ENC



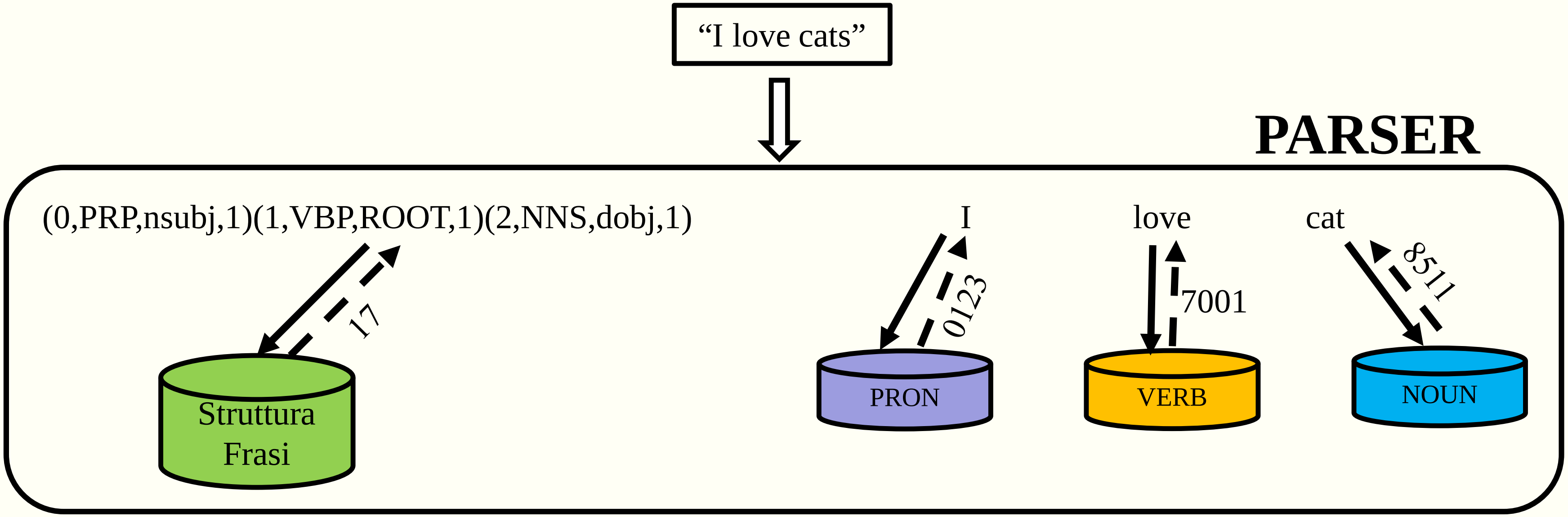
Il mio progetto – Schema ENC



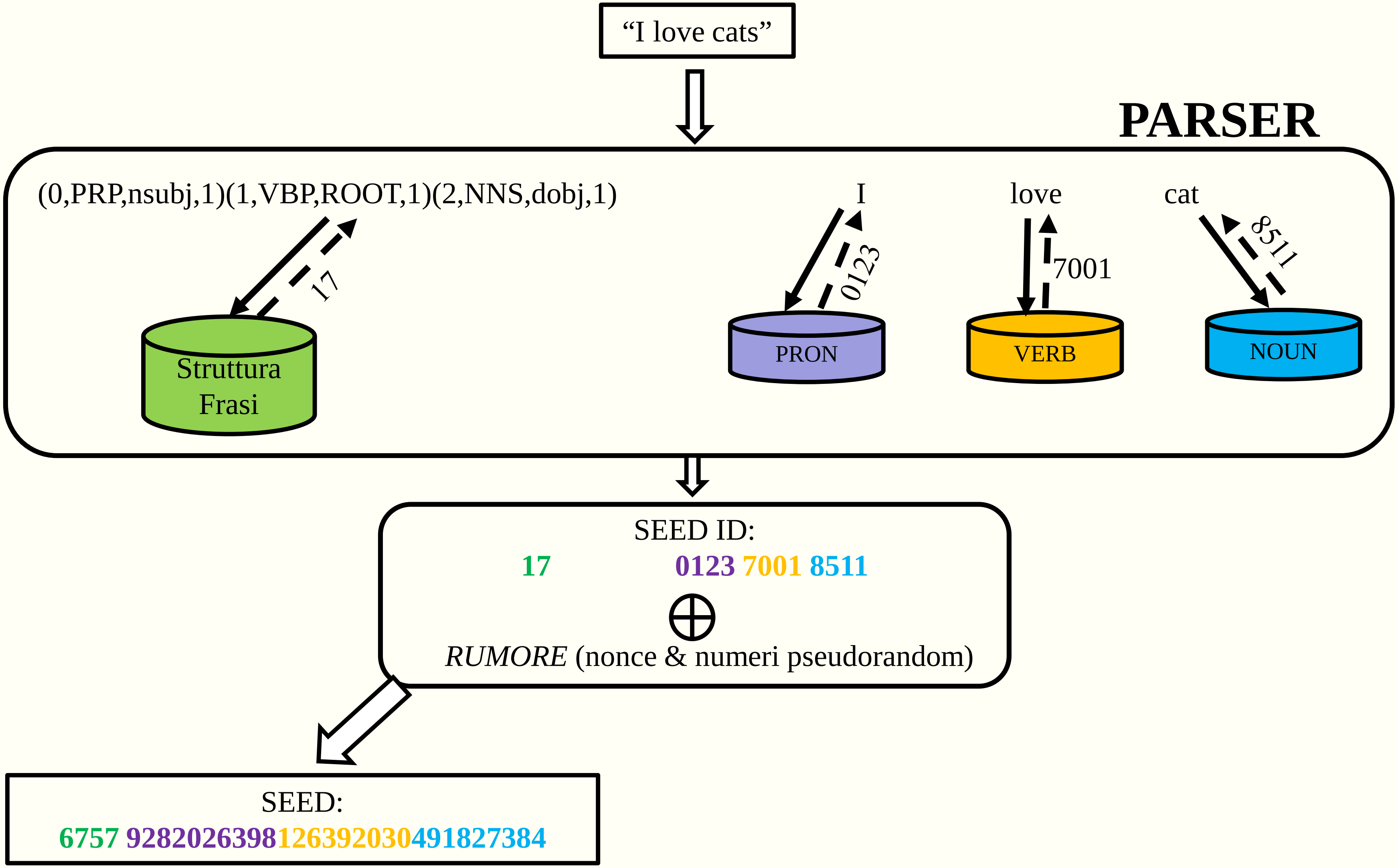
Il mio progetto – Schema ENC



Il mio progetto – Schema ENC Esempio



Il mio progetto – Schema ENC Esempio



“I love cats”

PARSER

(0,PRP,nsubj,1)(1,VBP,ROOT,1)(2,NNS,dobj,1)

SEED ID:

17 **0123 7001 8511**

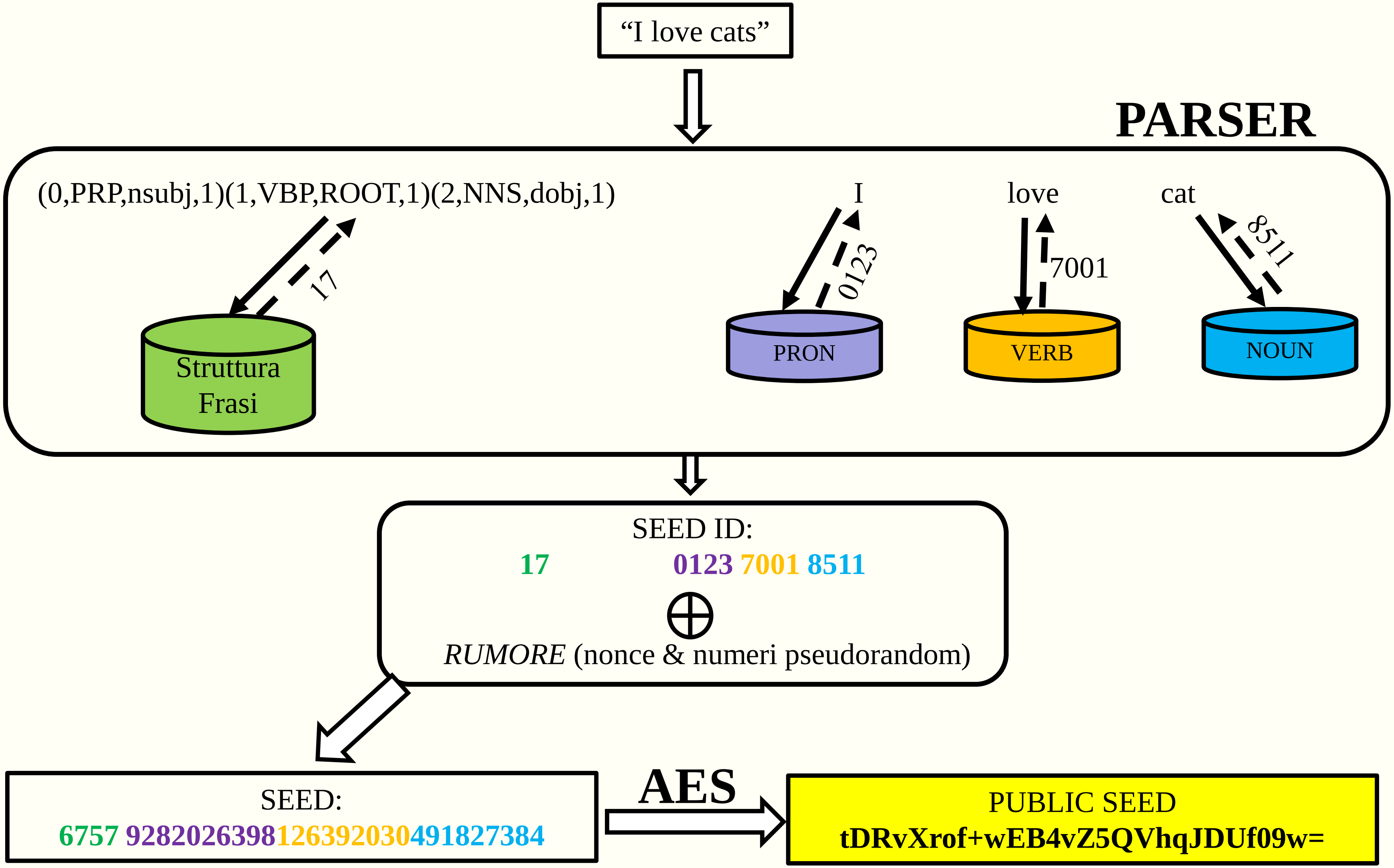
⊕

RUMORE (nonce & numeri pseudorandom)

SEED:

6757 9282026398126392030491827384

Il mio progetto – Schema ENC Esempio



"I love cats"

PARSER

(0,PRP,nsubj,1)(1,VBP,ROOT,1)(2,NNS,dobj,1)

17

Struttura Frasi

I

0123

PRON

love

7001

VERB

cat

8511

NOUN

SEED ID:

17 0123 7001 8511

⊕

RUMORE (nonce & numeri pseudorandom)

SEED:

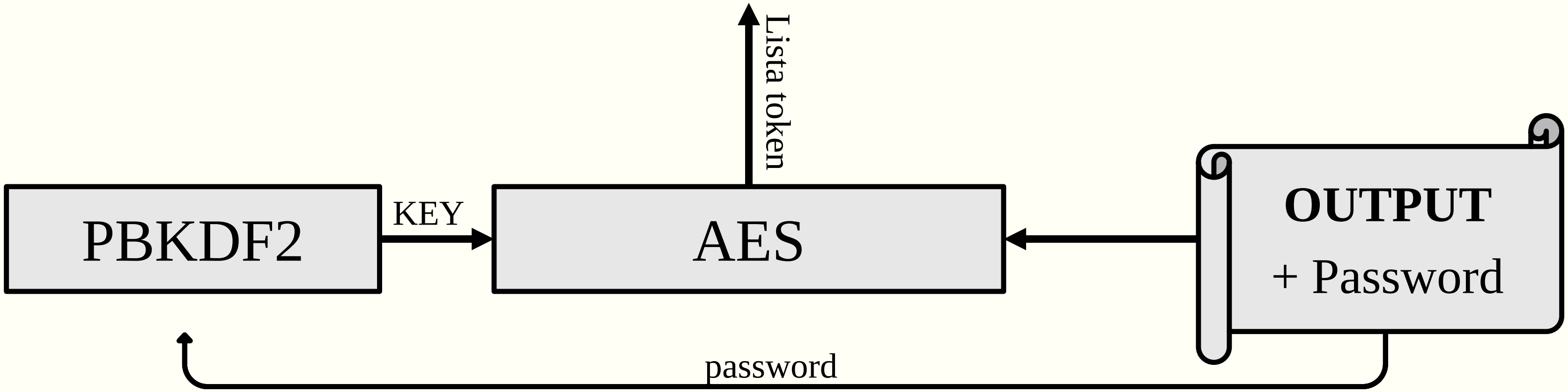
6757 9282026398126392030491827384

AES

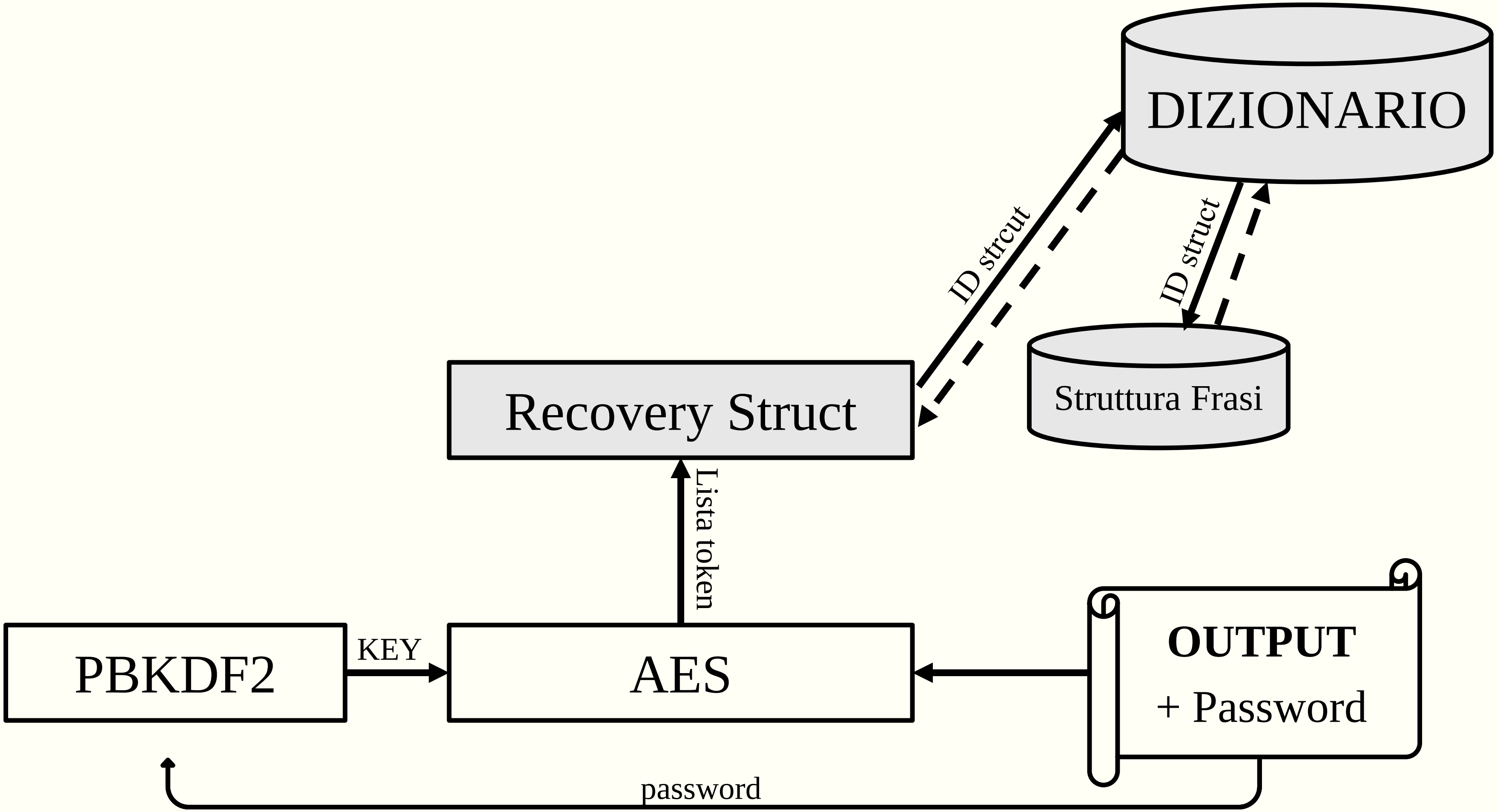
PUBLIC SEED

tDRvXrof+wEB4vZ5QVhqJDUf09w=

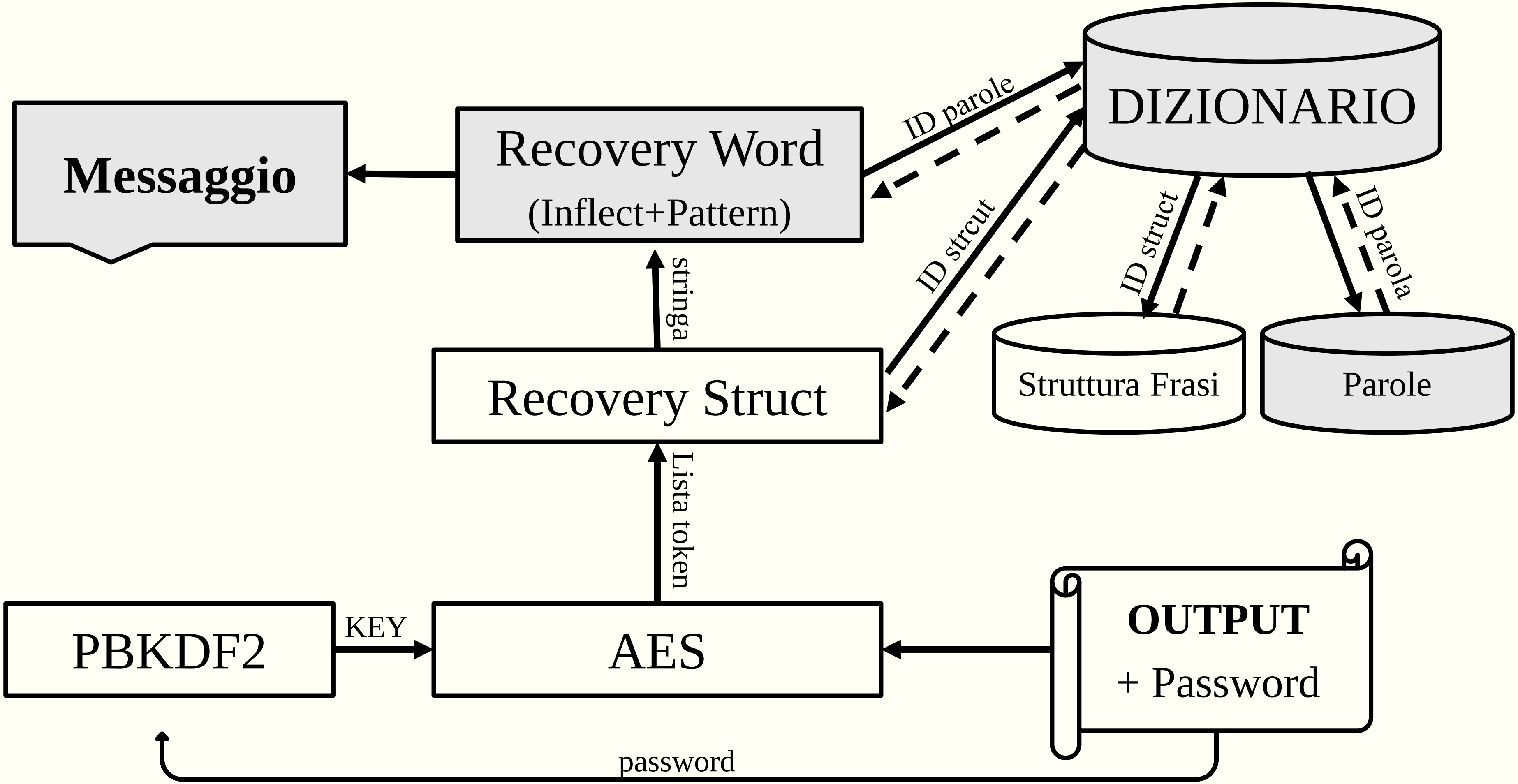
Il mio progetto – Schema DEC



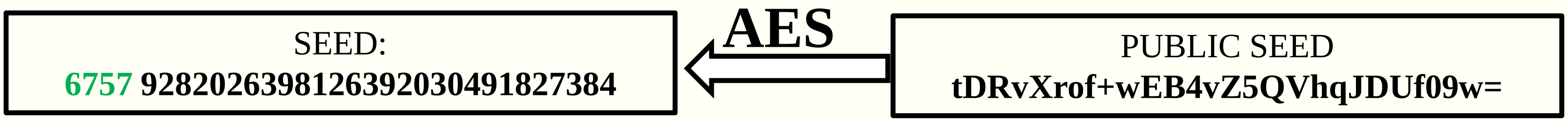
Il mio progetto – Schema DEC



Il mio progetto – Schema DEC Esempio



Il mio progetto – Schema DEC Esempio



SEED:

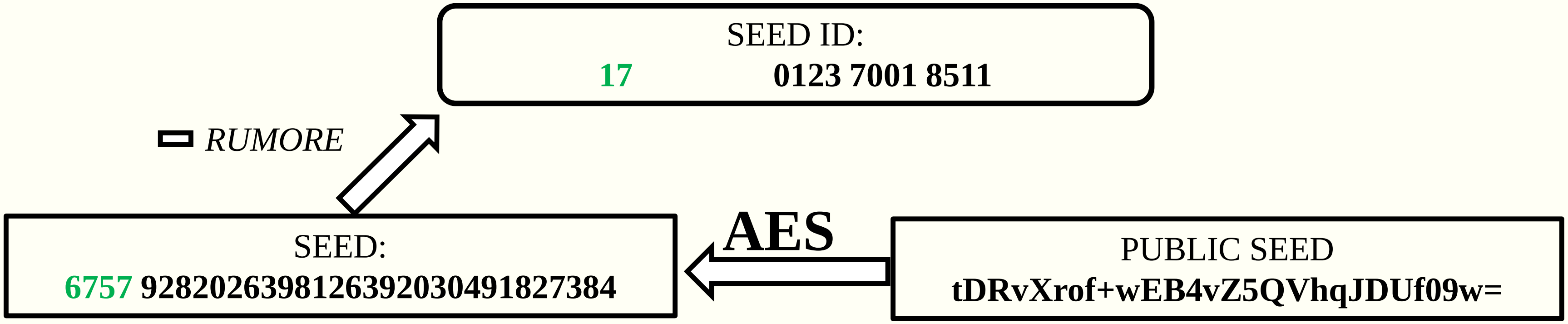
6757 **9282026398126392030491827384**

AES

PUBLIC SEED

tDRvXrof+wEB4vZ5QVhqJDUf09w=

Il mio progetto – Schema DEC Esempio



SEED ID:
17 0123 7001 8511

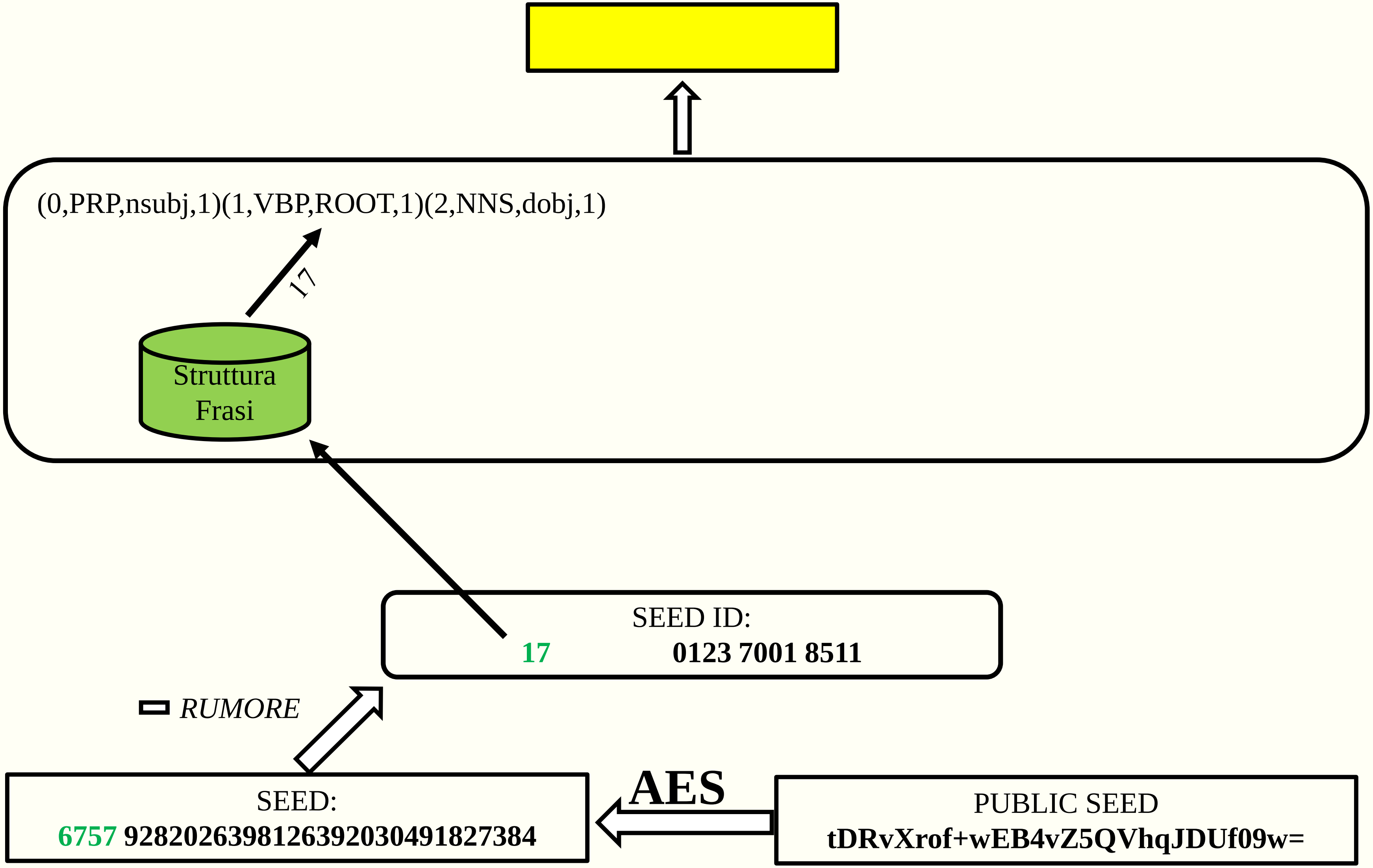
− *RUMORE*

SEED:
6757 92820263981263920304918273840

AES

PUBLIC SEED
tDRvXrof+wEB4vZ5QVhqJDUf09w=

Il mio progetto – Schema DEC Esempio



(0,PRP,nsubj,1)(1,VBP,ROOT,1)(2,NNS,dobj,1)

17

Struttura Frasi

SEED ID:

17 0123 7001 8511

▭ *RUMORE*

SEED:

6757 9282026398126392030491827384

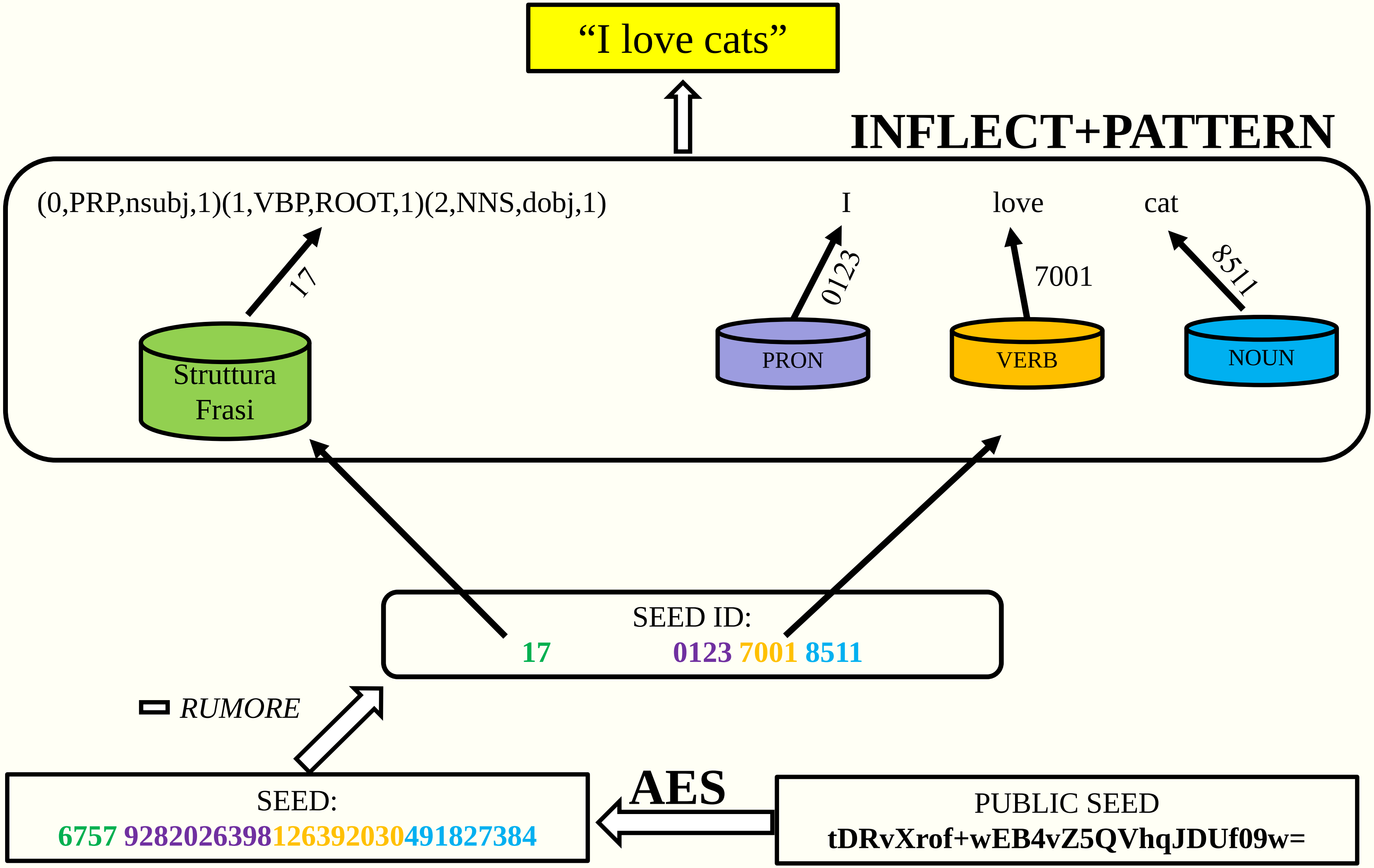
AES

PUBLIC SEED

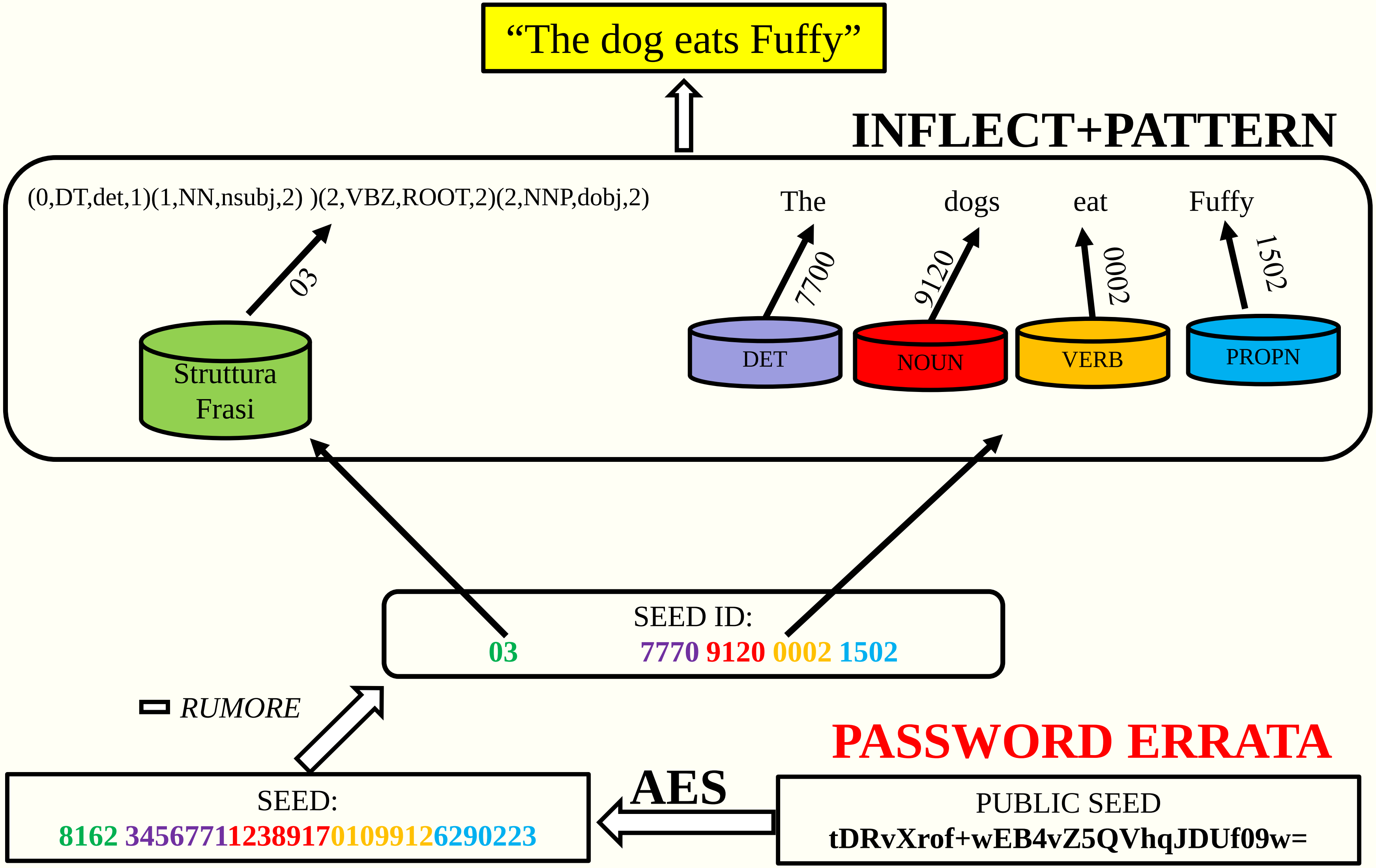
tDRvXrof+wEB4vZ5QVhqJDUf09w=

UNIVERSITÀ DEGLI STUDI DI BRESCIA

Il mio progetto – Schema DEC Esempio



Il mio progetto – Schema DEC Esempio



“The dog eats Fuffy”

INFLECT+PATTERN

(0,DT,det,1)(1,NN,nsubj,2))(2,VBZ,ROOT,2)(2,NNP,dobj,2)

SEED ID:
03 7770 9120 0002 1502

▭ *RUMORE*

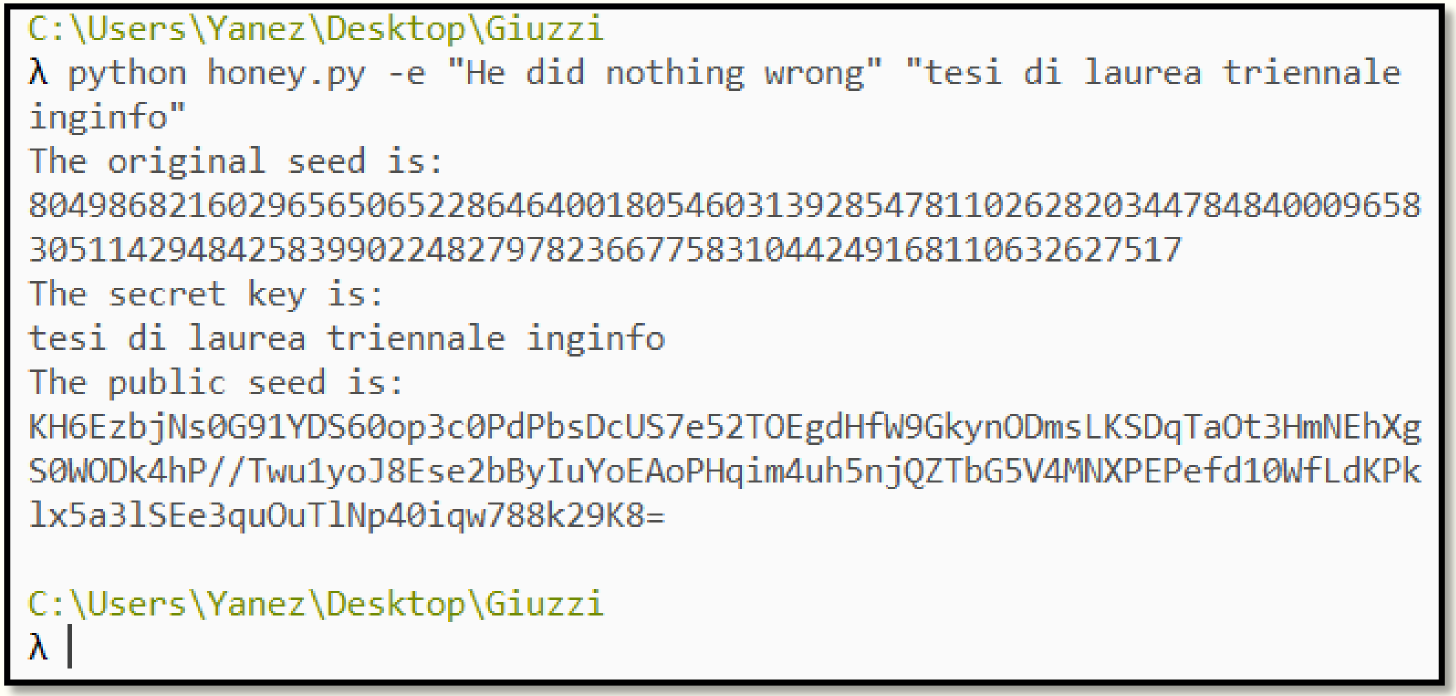
PASSWORD ERRATA

SEED:
8162 3456771123891701099126290223

AES

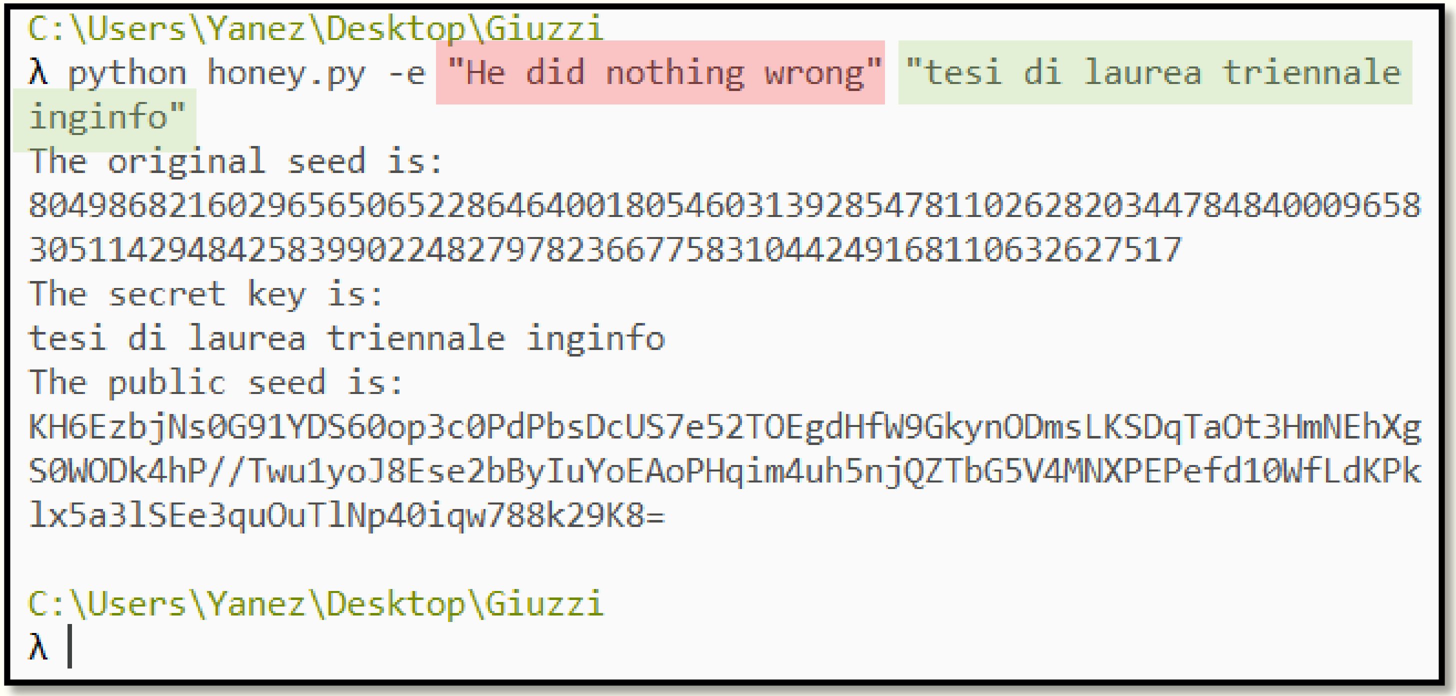
PUBLIC SEED
tDRvXrof+wEB4vZ5QVhqJDUf09w=

Il mio progetto – Esempio ENC



```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -e "He did nothing wrong" "tesi di laurea triennale
inginfo"
The original seed is:
80498682160296565065228646400180546031392854781102628203447848400096583
05114294842583990224827978236677583104424916811063262751 7
```

Il mio progetto – Esempio ENC

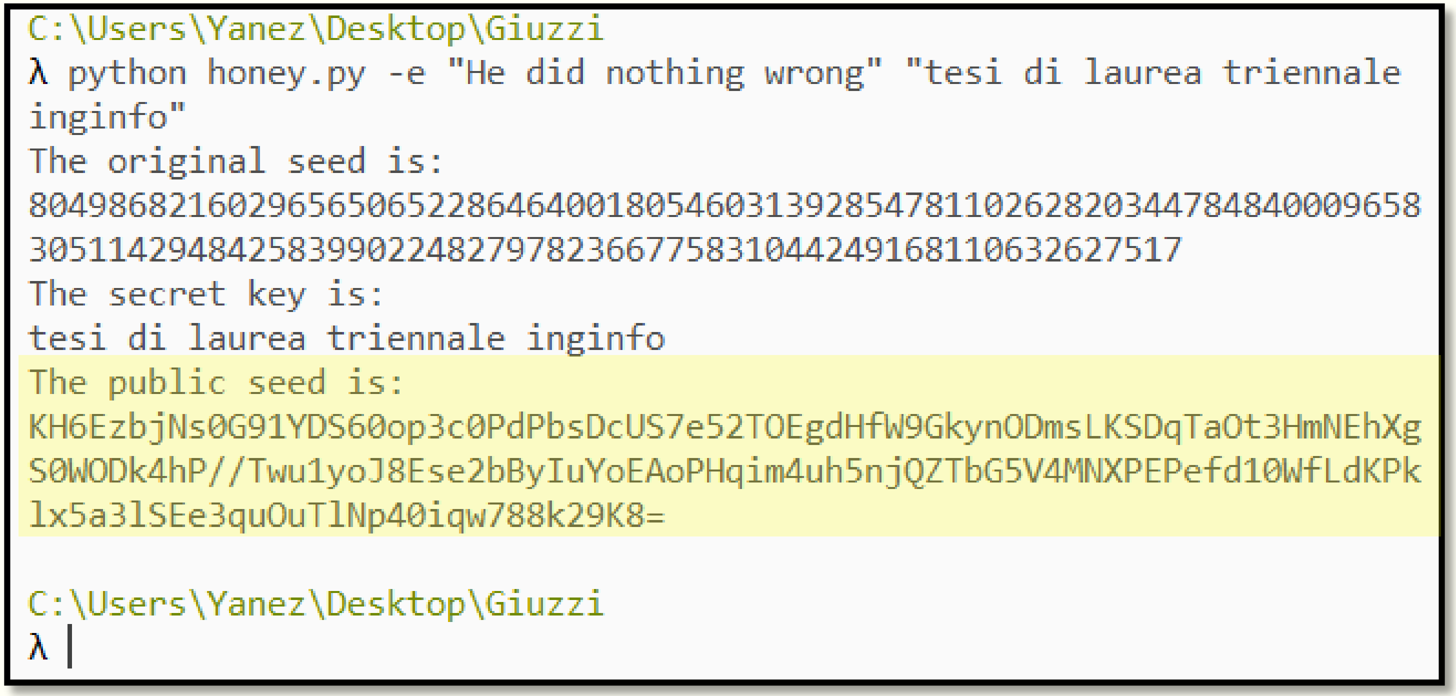


```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -e "He did nothing wrong" "tesi di laurea triennale
inginfo"
The original seed is:
8049868216029656506522864640018054603139285478110262820344784840009658
30511429484258399022482797823667758310442491681106327517
The secret key is:
tesi di laurea triennale inginfo
The public seed is:
KH6EzbjNs0G91YDS60op3c0PdPbsDcUS7e52TOEgdHfW9GkynODmsLKSDqTaOt3HmNEhXg
S0WODk4hP//Twu1yoJ8Ese2bByIuYoEAoPHqim4uh5njQZTbG5V4MNXPEPefd10WfLdKPk
lx5a3lSEe3quOuTlNp40iqw788k29K8=

C:\Users\Yanez\Desktop\Giuzzi
λ
```

UNIVERSITÀ DEGLI STUDI DI BRESCIA

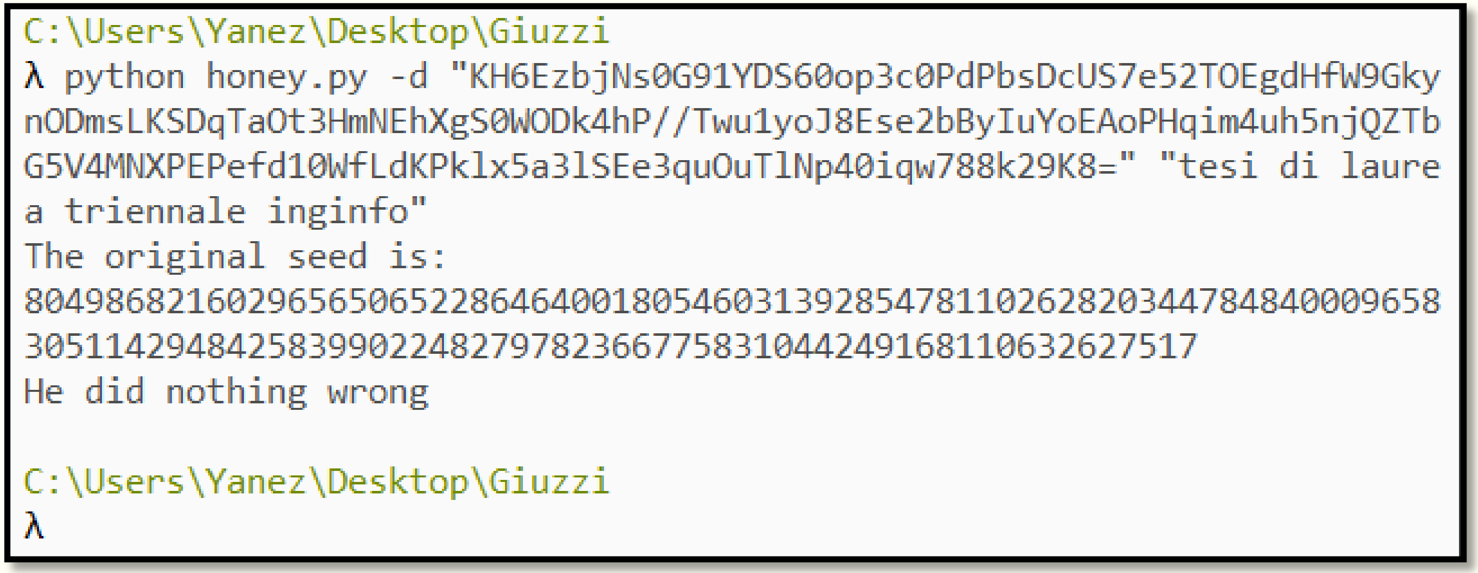
Il mio progetto – Esempio ENC



```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -e "He did nothing wrong" "tesi di laurea triennale
inginfo"
The original seed is:
8049868216029656506522864640018054603139285478110262820344784840009658
3051142948425839902248279782366775831044249168110632627517
The secret key is:
tesi di laurea triennale inginfo
The public seed is:
KH6EzbjNs0G91YDS60op3c0PdPbsDcUS7e52TOEgdHfW9GkynODmsLKSDqTaOt3HmNEhXg
S0WODk4hP//Twu1yoJ8Ese2bByIuYoEAoPHqim4uh5njQZTbG5V4MNXPEPefd10WfLdKPk
lx5a3lSEe3quOuTlNp40iqw788k29K8=

C:\Users\Yanez\Desktop\Giuzzi
λ |
```

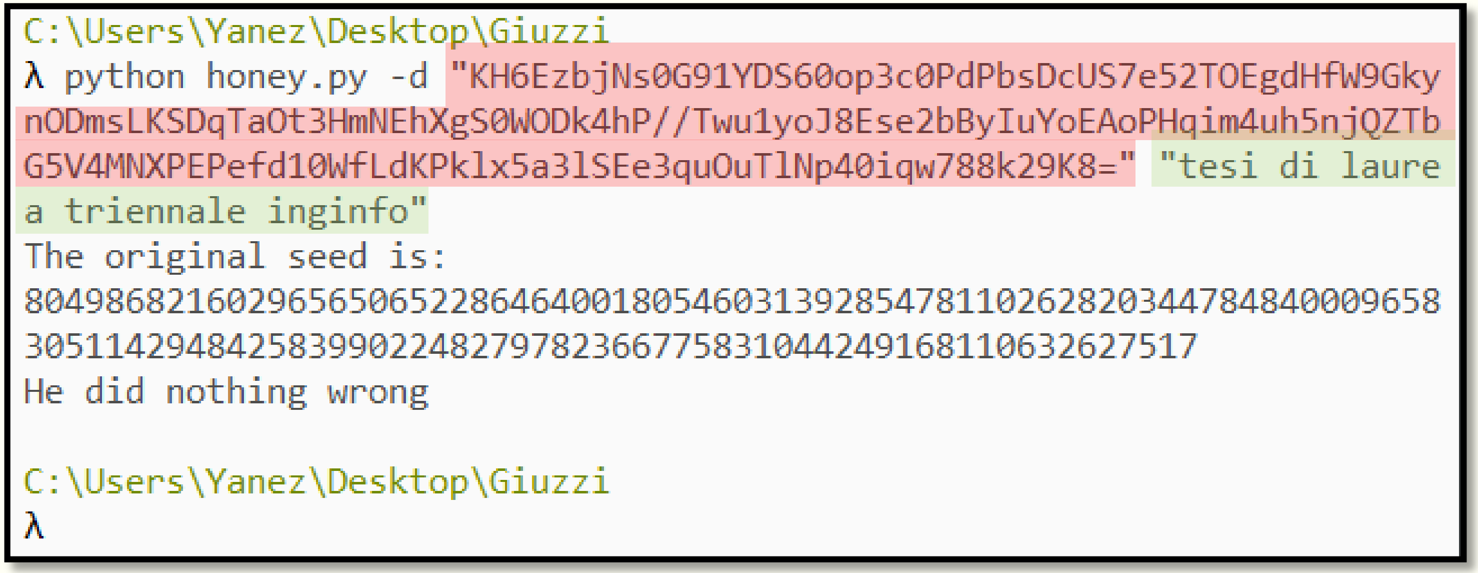
Il mio progetto – Esempio DEC



```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -d "KH6EzbjNs0G91YDS60op3c0PdPbsDcUS7e52TOEgdHfW9Gky
nODmsLKSDqTaOt3HmNEhXgS0WODk4hP//Twu1yoJ8Ese2bByIuYoEAoPHqim4uh5njQZTb
G5V4MNXPEPefd10WfLdKPklx5a31SEe3quOuTlNp40iqw788k29K8=" "tesi di laure
a triennale inginfo"
The original seed is:
8049868216029656506522864640018054603139285478110262820344784840009658
3051142948425839902248279782366775831044249168110632627517
He did nothing wrong

C:\Users\Yanez\Desktop\Giuzzi
λ
```

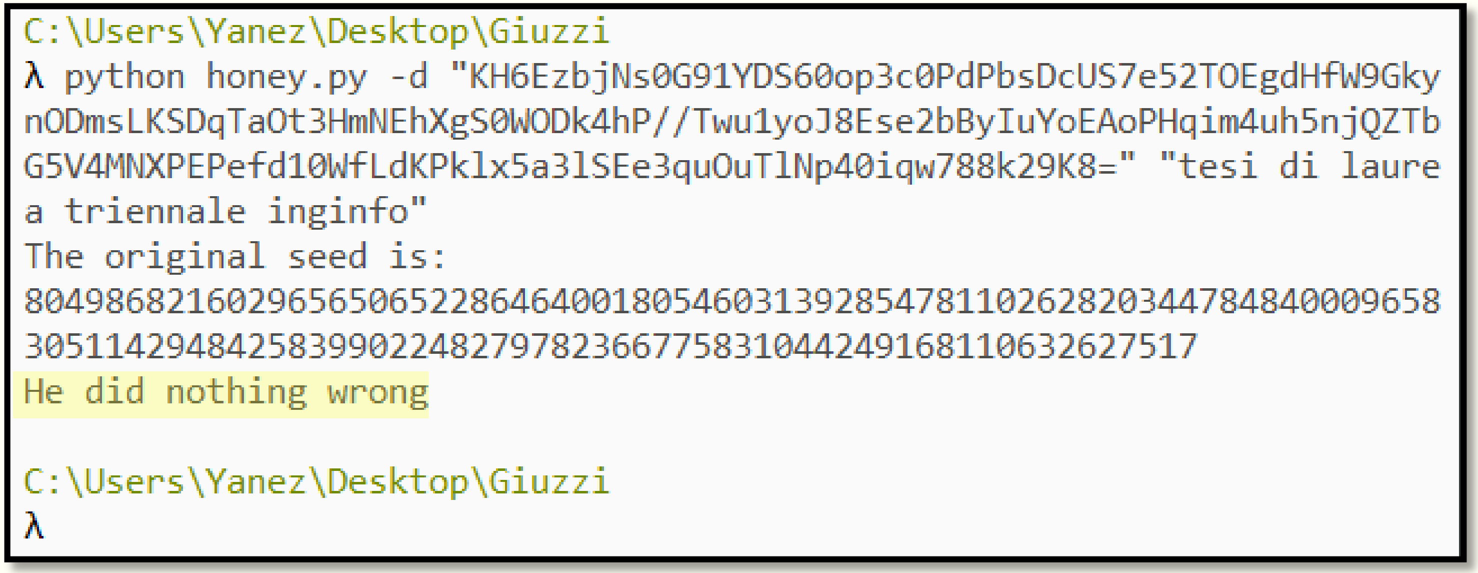
Il mio progetto – Esempio DEC



```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -d "KH6EzbjNs0G91YDS60op3c0PdPbsDcUS7e52TOEgdHfW9Gky
nODmsLKSDqTaOt3HmNEhXgS0WODk4hP//Twu1yoJ8Ese2bByIuYoEAoPHqim4uh5njQZTb
G5V4MNXPEPefd10WfLdKPklx5a31SEe3quOuTlNp40iqw788k29K8=" "tesi di laure
a triennale inginfo"
The original seed is:
8049868216029656506522864640018054603139285478110262820344784840009658
3051142948425839902248279782366775831044249168110632627517
He did nothing wrong

C:\Users\Yanez\Desktop\Giuzzi
λ
```

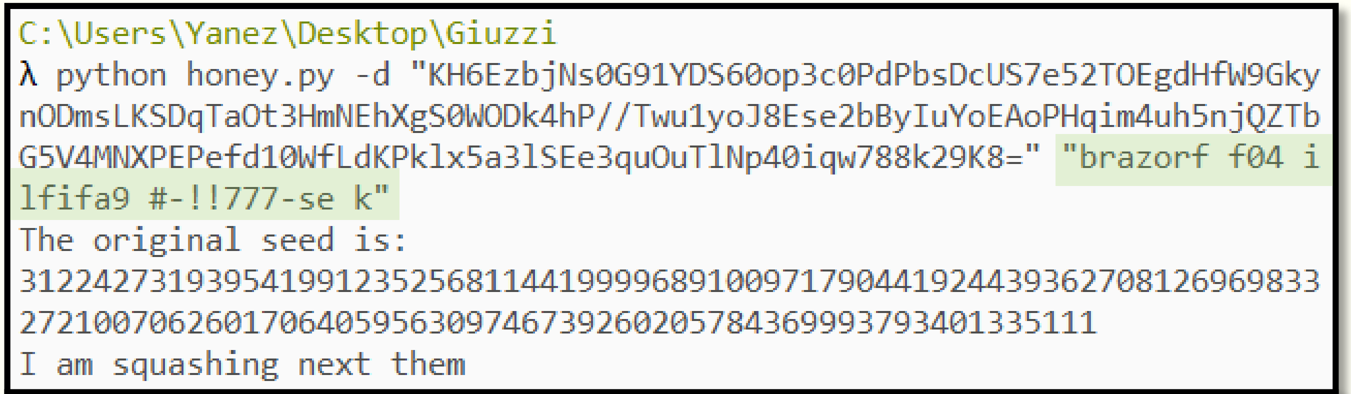
Il mio progetto – Esempio DEC



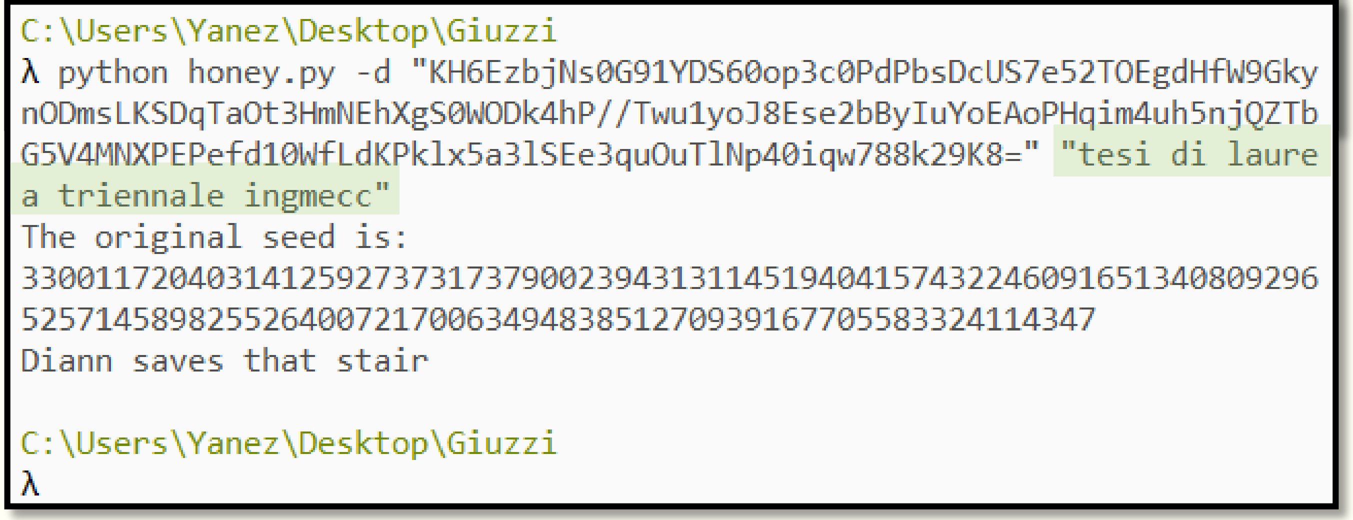
```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -d "KH6EzbjNs0G91YDS60op3c0PdPbsDcUS7e52TOEgdHfW9Gky
nODmsLKSDqTaOt3HmNEhXgS0WODk4hP//Twu1yoJ8Ese2bByIuYoEAoPHqim4uh5njQZTb
G5V4MNXPEPefd10WfLdKPklx5a3lSEe3quOuTlNp40iqw788k29K8=" "tesi di laure
a triennale inginfo"
The original seed is:
80498682160296565065228646400180546031392854781102628203447848400009658
30511429484258399022482797823667758310442491681106326275 17
He did nothing wrong

C:\Users\Yanez\Desktop\Giuzzi
λ
```

Il mio progetto – Esempio PSW Errata



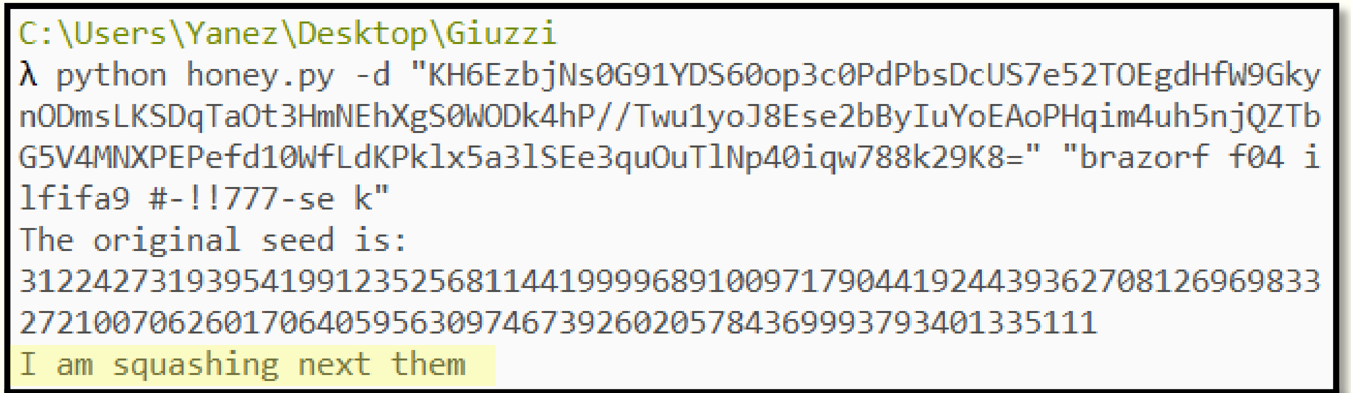
```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -d "KH6EzbjNs0G91YDS60op3c0PdPbsDcUS7e52TOEgdHfW9Gky
nODmsLKSDqTaOt3HmNEhXgS0WODk4hP//Twu1yoJ8Ese2bByIuYoEAoPHqim4uh5njQZTb
G5V4MNXPEPefd10WfLdKPklx5a3lSEe3quOuTlNp40iqw788k29K8=" "brazorf f04 i
lfifa9 #-!!777-se k"
The original seed is:
3122427319395419912352568114419999689100971790441924439362708126969833
2721007062601706405956309746739260205784369993793401335111
I am squashing next them
```



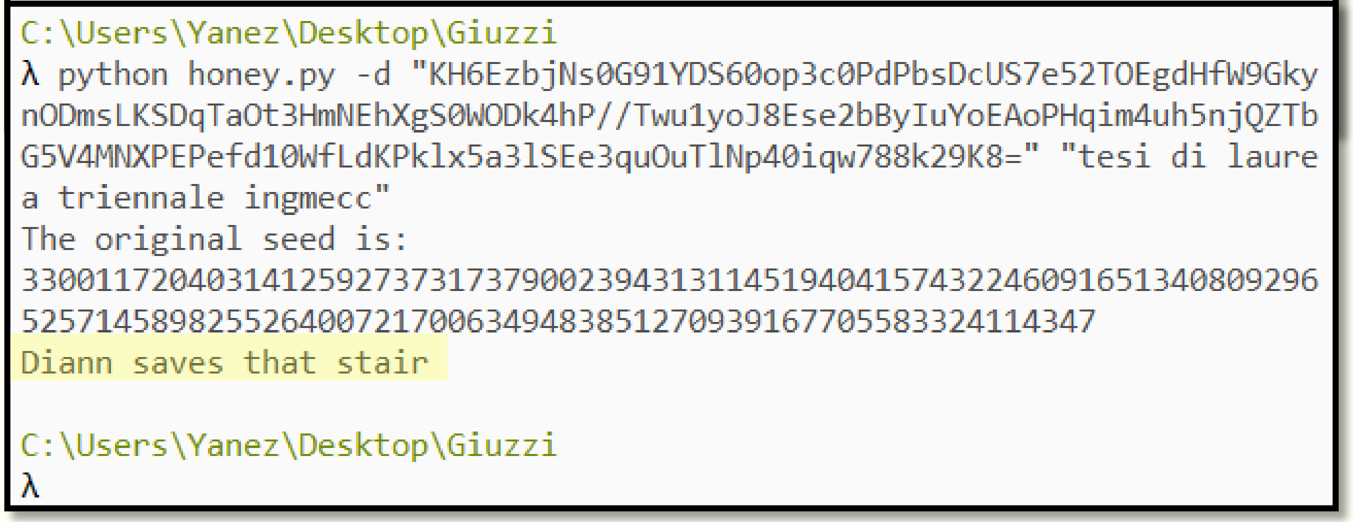
```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -d "KH6EzbjNs0G91YDS60op3c0PdPbsDcUS7e52TOEgdHfW9Gky
nODmsLKSDqTaOt3HmNEhXgS0WODk4hP//Twu1yoJ8Ese2bByIuYoEAoPHqim4uh5njQZTb
G5V4MNXPEPefd10WfLdKPklx5a3lSEe3quOuTlNp40iqw788k29K8=" "tesi di laure
a triennale ingmecc"
The original seed is:
3300117204031412592737317379002394313114519404157432246091651340809296
5257145898255264007217006349483851270939167705583324114347
Diann saves that stair

C:\Users\Yanez\Desktop\Giuzzi
λ
```

Il mio progetto – Esempio PSW Errata



```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -d "KH6EzbjNs0G91YDS60op3c0PdPbsDcUS7e52TOEgdHfW9Gky
nODmsLKSDqTaOt3HmNEhXgS0WODk4hP//Twu1yoJ8Ese2bByIuYoEAoPHqim4uh5njQZTb
G5V4MNXPEPefd10WfLdKPklx5a3lSEe3quOuTlNp40iqw788k29K8=" "brazorf f04 i
lfifa9 #-!!777-se k"
The original seed is:
3122427319395419912352568114419999689100971790441924439362708126969833
2721007062601706405956309746739260205784369993793401335111
I am squashing next them
```



```
C:\Users\Yanez\Desktop\Giuzzi
λ python honey.py -d "KH6EzbjNs0G91YDS60op3c0PdPbsDcUS7e52TOEgdHfW9Gky
nODmsLKSDqTaOt3HmNEhXgS0WODk4hP//Twu1yoJ8Ese2bByIuYoEAoPHqim4uh5njQZTb
G5V4MNXPEPefd10WfLdKPklx5a3lSEe3quOuTlNp40iqw788k29K8=" "tesi di laure
a triennale ingmecc"
The original seed is:
3300117204031412592737317379002394313114519404157432246091651340809296
5257145898255264007217006349483851270939167705583324114347
Diann saves that stair

C:\Users\Yanez\Desktop\Giuzzi
λ
```

Il mio progetto – Future Implementazioni

- **Eliminare Dizionari delle frasi**
  - Dizionari relazionati (Contesto) – Datamuse *[11]*
  - Dizionario synset (sinonimi) – Wordnet *[12]*
- **Eliminare Dizionario delle strutture grammaticali**
- **Frasi composte da più periodi**

LINK

“Honey Encryption: Security Beyond the Brute-Force Bound” *di Ari Juels e Thomas Ristenpart*

https://eprint.iacr.org/2014/155.pdf

[1] Mimoso, Michael (29 Jan 2014). **"Honey Encryption Tricks Hackers with Decryption Deceiption“**

https://threatpost.com/honey-encryption-tricks-hackers-with-decryption-deception/103950/

[2] Nirvan Tyagi, Daniel Zuo, Jessica Wang, Kevin Wen. **Honey Encryption for Credit Card Example**

https://github.com/danielzuot/honeyencryption

[3] **“Protecting Private Data by Honey Encryption”** *di Wei Yin, Jadwiga Indulska e Hongjian Zhou*

https://www.hindawi.com/journals/scn/2017/6760532/

[4] **“Implementing the Honey Encryption for Securing Public Cloud Data Storage”** *di Edwin Mok, Azman Samsudin e Soo-Fun Tan*

https://pdfs.semanticscholar.org/b73e/6edd1b5cc330ba8c10c1bfbed5cc9ea25e8c.pdf

LINK

[5] **“Honey Chatting”** *di Joo-Im Kim e Ji Won Yoon*

https://ieeexplore.ieee.org/document/7472064

[6] **“A Novel Approach for the Adaptation of Honey Encryption to Support Natural Language Message”** *di Abiodun Esther Omolara, Aman Jantan, Oludare Isaac Abiodun e Howard Eldon Poston*

http://www.iaeng.org/publication/IMECS2018/IMECS2018_pp134-139.pdf

[7] **spaCy** - Industrial-Strength Natural Language Processing IN PYTHON

https://spacy.io/

[8] **The Stanford Parser: A statistical parser**

https://nlp.stanford.edu/software/lex-parser.shtml

[9] **Pattern.en**

https://www.clips.uantwerpen.be/pages/pattern-en

[10] **Inflect project**

https://github.com/jazzband/inflect

[11] **Datamuse**

https://www.datamuse.com/

[12] **WordNet** - A Lexical Database for English

https://wordnet.princeton.edu/