Cenni di crittografia e crittoanalisi

•••

Percorsi per le competenze trasversali e l'orientamento

Andrea Zubenko - Università degli studi di Milano

Crittografia

Kryptós (nascosto) + *graphia* (scrittura)

Come nascondo il testo?

Testo + tecnica di cifratura + chiave

- Simmetrica
- Asimmetrica
- Quantistica

Il cifrario atbash

L'origine di questo cifrario si puó trovare nella bibbia (babele -> sheshakh)

La prima lettera dell'alfabeto viene sostituita con l'ultima, la seconda con la penultima e cosí via

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

Alternanza -> Zogvimzmaz

Tecnicamente: **cifrario a sostituzione monoalfabetica**

Cifrario di Cesare

Ogni lettera viene sostituita con quella che si trova dopo un certo numero di posizioni nell'alfabeto... o anche prima

Chiave: di quanto bisogna spostarsi

```
Chiaro:  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
Cifrato: 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
```

In generale

Si tratta di **cifrari a sostituzione monoalfabetica**

Forma piú generale: cifrari a permutazione

Chiave: l’intera permutazione

Cifrario di Vigenère

Si tratta di un cifrario a sostituzione polialfabetica

```
Chiaro:  C I A O A T U T T I

Chiave:  V E R M E V E R M E

Cifrato: X M R A E O Y K F M
```

Crittoanalisi

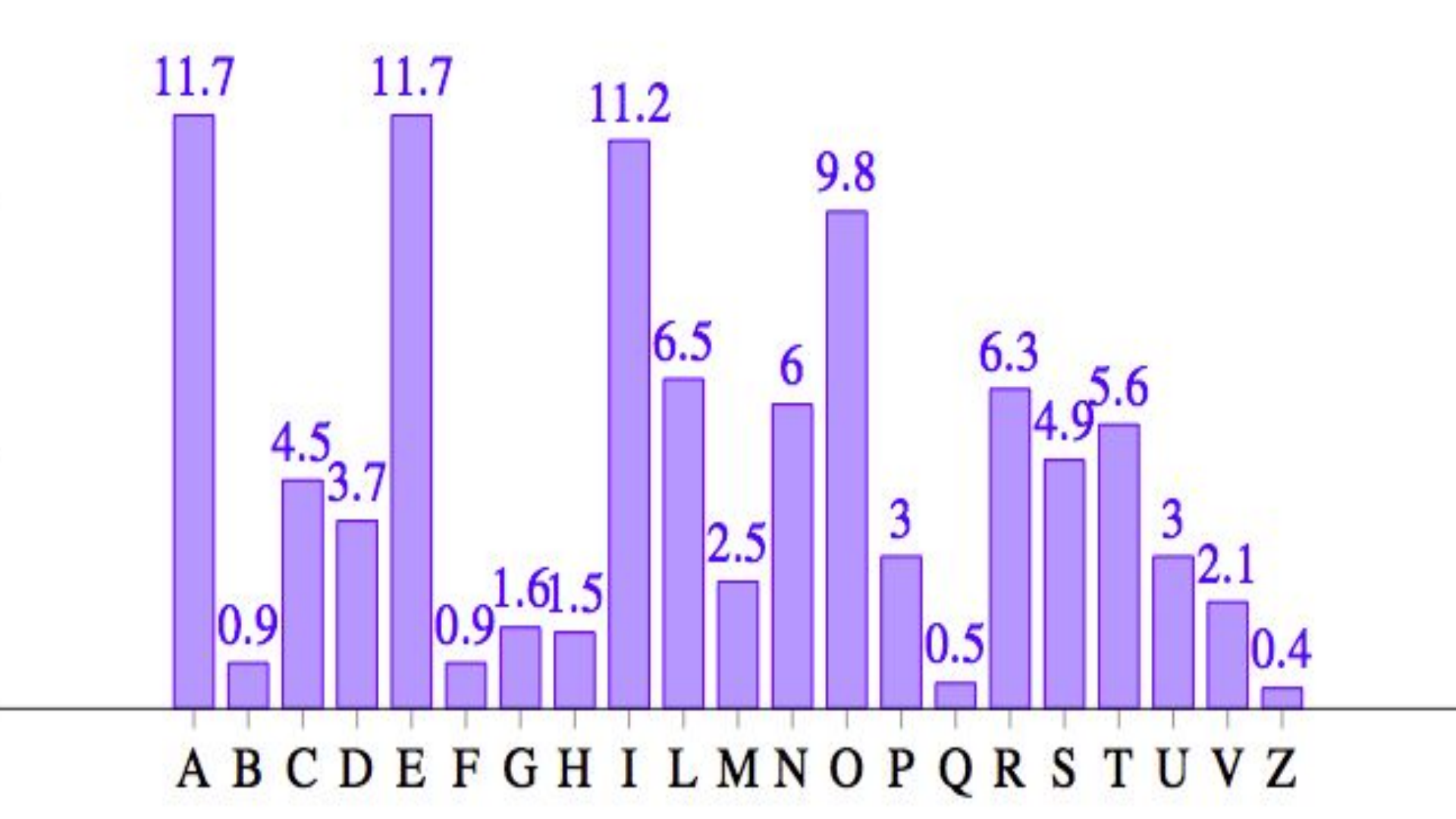
Kryptós (nascosto) + *analýein (scomporre)*

Hlml Zmwivz, irfhxrgv z xzkrinr?

Hlml Amwiva, irfhxrgv a xakrinr?

Hlnl Andrea, rrfhxrge a xakrrnr?

Sono Andrea, riuscite a capirmi?


11.7
0.9
4.5
3.7
11.7
0.9
1.6
1.5
11.2
6.5
2.5
6
9.8
3
0.5
6.3
4.9
5.6
3
2.1
0.4
A B C D E F G H I L M N O P Q R S T U V Z

ESERCIZI!

http://malchiodi.di.unimi.it/crittografia/

Ringrazio Dario Malchiodi per il materiale da cui ho preso spunto per questa presentazione