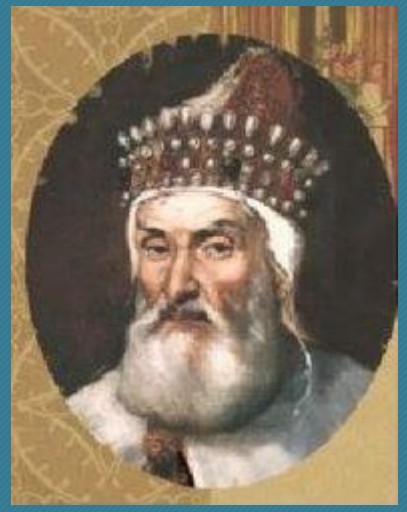
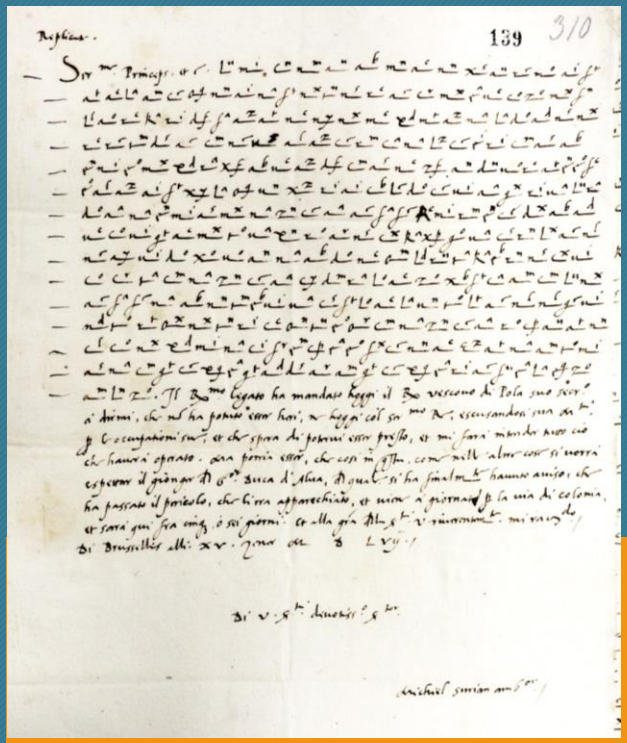
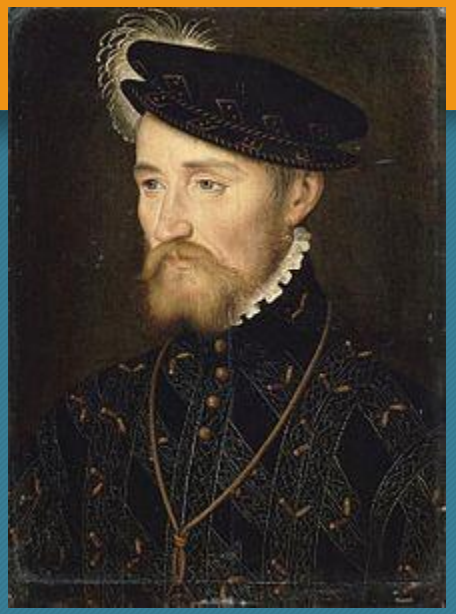




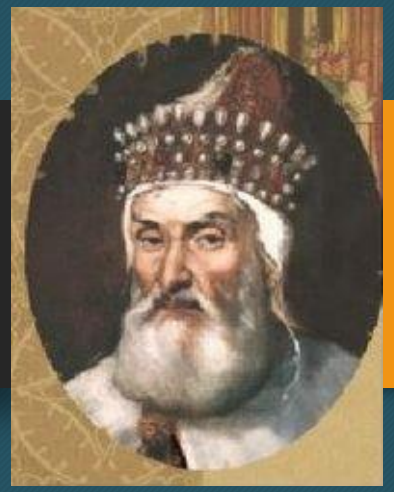
Crittografia a Venezia tra matematica e storia



La Crittografia come matematica applicata

La Crittografia come strumento di ricerca storica

Un dispaccio da Bruxelles 15-1-1558 (o 1557?)

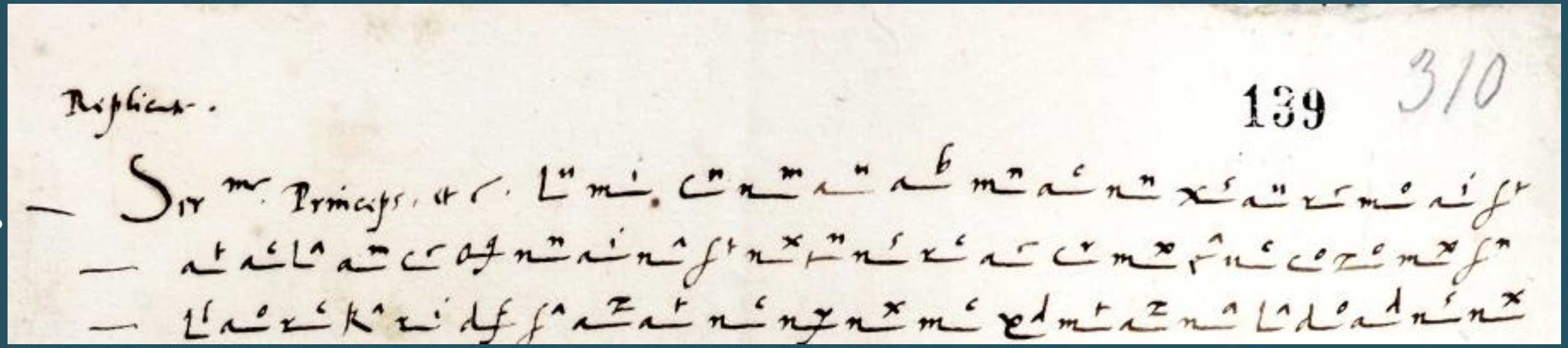


Replica.

139 310

Un dispaccio deciferato

Lu mi cn nm au ab mn ac nn xs au re mo ai ft at ac La am ce oq nn ai na ft quest a ma tti na e spa r sa u na uo ce per la co r te se n za sa per si la
Questa mattina è sparsa una uoce per la corte senza sapersi la

- 

I nomenclatori

Lu mi cn nm au ab mn ac nn xs au re mo ai ft at ac La am ce oq nn ai na ft
quest a ma tti na e spa r sa u na uo ce per la co r te se n za sa per si la
Questa mattina è sparsa una uoce per la corte senza sapersi la

Nomenclatore

Cifrario per sostituzione: per lettera, per sillaba, per parole parziali o intere

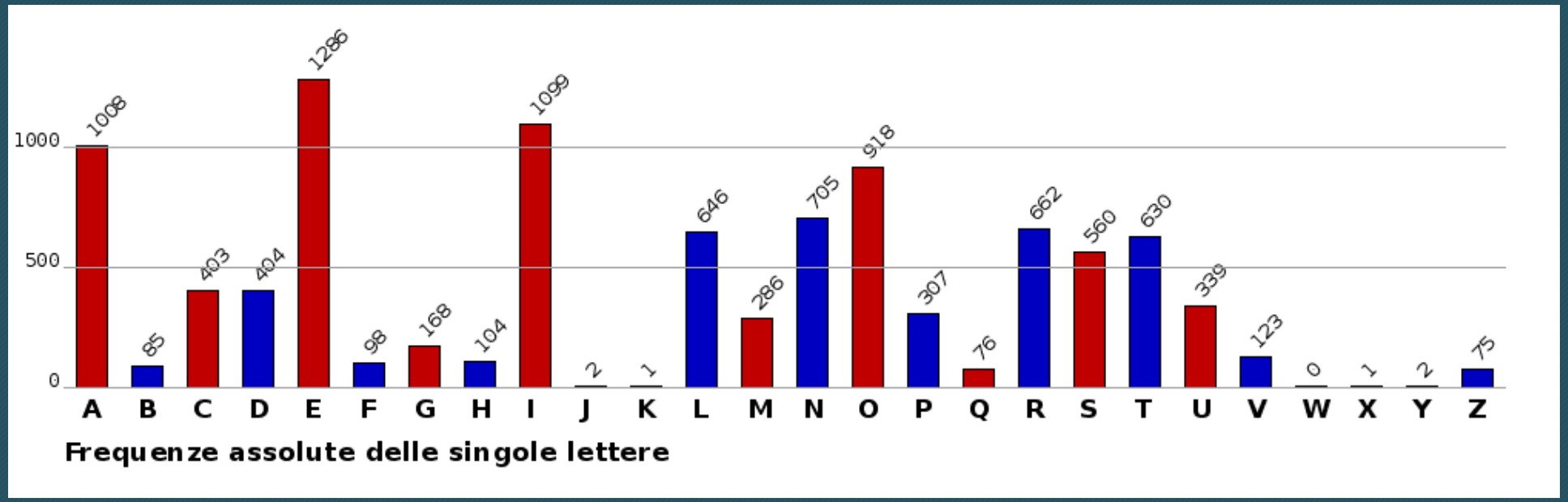
Nella cancelleria del Doge i dispacci venivano decifrati da personale addestrato

Il testo decifrato

- Questa mattina è sparsa una uoce per la corte senza sapersi la origine che Franzesi sono andati sopra Guines et perché il loco è molto picciolo si teme ragioneuolmente che non potrà far longa resistenza et non ui è modo di soccorrerlo perché non ui è essercito in esser ne comodita di farlo per la streteza del tempo et per mancamento de danari et con questo medesimo auiso si intende che il conte d Agamon il quale era andato uerso li confini come gia scrissi con quelle gente che ha potuto metter insieme e stato rotto et sualegiato da Franzesi et non si intende anchor altro particulare se non questo come il conte si e saluato con quella parte delli sui come ha hauuto caualli migliori et più presti di Anglia non si intende niuna cosa il che da occasione ad ogniuno di pensar mal cosi se li auisi non uengono ueramente come se uengono et che siano tenuti secreti

Crittografia e statistica

- Nella crittografia classica l'arma più potente per il crittoanalista è la statistica; ogni lingua ha un distribuzione statistica caratteristica; qui sotto quella della lingua italiana.



Crittografia, relazioni, funzioni

- I cifrari sono **funzioni** o meglio **relazioni** tra l'insieme dei messaggi in chiaro (dominio) e l'insieme dei messaggi cifrati (codominio).
- In teoria ci aspetteremmo una corrispondenza biunivoca ma non sempre è così.
- Nella crittografia classica, come la precedente, la relazione chiaro-> cifrato non è mai biunivoca.

Crittografia: funzioni?

- La funzione cifrante non è ovunque definita: spazi, segni di interpunzione non vengono cifrati.
- La funzione cifrante non è univoca; cifratura per ***omofoni***, una stessa lettera si può cifrare con segni diversi, per confondere la statistica.
- La funzione cifrante non è suriettiva, alcuni segni cifranti, detti ***nulle***, non hanno corrispondente in chiaro, sempre per confondere.
- La funzione cifrante non è iniettiva, alcuni segni cifranti, detti ***polifoni***, hanno più significati; da risolvere in base al contesto (raro)