

## Phvvdlln vhluzn: od funzzrludind nq muhfr h nq odznqr.

«Ne ferisce più la penna che la spada»: in alcuni episodi della storia greca e romana questo adagio dovette essere preso terribilmente alla lettera. Molti grandi strateghi si affidarono infatti al potere delle parole e dei numeri per comunicare con gli alleati alle spalle dei nemici, costruendo codici segreti per crittografare ordini o soffiare. Potevano così contare su un'arma assai più sottile e imprevedibile di quelle fatte di ferro o bronzo: il linguaggio. La storiografia ci riporta numerosi esempi di sistemi per cifrare i messaggi; i tre brani proposti illustrano l'invenzione di due diversi codici che ebbero molta fortuna nella storia della crittografia e che furono utilizzati anche in altre circostanze ed epoche storiche.

### 1. Polibio, *Storie X*, 45, 6-12:

In questo passo delle *Storie* Polibio presenta un cifrario utile per trasmettere a distanza dei messaggi per mezzo di fiaccole. Non si tratta di un vero e proprio codice segreto; il sistema assomiglia di più a una sorta di telegrafo luminoso. È necessario però che mittente e ricevente siano in possesso di tabelle di decodifica costruite allo stesso modo; queste ultime possono anche essere cifrate, per esempio cambiando l'ordine delle lettere nelle tabelle stesse. Il cifrario, perfezionato dallo stesso storico greco e passato perciò alla storia come “scacchiera di Polibio”, era impiegato in guerra per trasmettere comunicazioni urgenti.

Ὁ δὲ τελευταῖος (τρόπος), ἐπινοηθεὶς διὰ Κλεοξένου καὶ Δημοκλείτου, τυχῶν δὲ τῆς ἐξεργασίας δι' ἡμῶν, (πάντη πάντως) μὲν ἔστιν ὀρισμένος καὶ πᾶν τὸ κατεπεῖγον δυνάμενος ἀκριβῶς **διασαφεῖν**, κατὰ δὲ τὸν χειρισμὸν ἐπιμελείας **δεῖ** καὶ παρατηρήσεως ἀκριβεστέρας. ἔστι δὲ τοιοῦτος. τὸ τῶν στοιχείων πλῆθος ἐξῆς **δεῖ λαμβάνοντας** διελεῖν εἰς πέντε μέρη κατὰ πέντε γράμματα. **λείπει** δὲ τὸ τελευταῖον ἐνὶ στοιχείῳ· τοῦτο δ' οὐ βλάπτει πρὸς τὴν χρείαν. μετὰ δὲ ταῦτα πλατεῖα **παρεσκευάσθαι** πέντε **τοὺς μέλλοντας** ἀποδιδόναι τὴν πυρσεῖαν ἀλλήλοις ἑκατέρους καὶ γράψαι τῶν μερῶν ἐξῆς εἰς ἕκαστον πλατεῖον, κᾶπειτα συνθέσθαι πρὸς αὐτοὺς διότι τοὺς μὲν πρώτους ἀρεῖ πυρσοὺς ὁ μέλλων σημαίνειν ἅμα καὶ δύο καὶ μενεῖ μέχρις ἂν ὁ ἕτερος ἀνταίρη. τοῦτο δ' ἔσται χάριν τοῦ διὰ ταύτης τῆς πυρσεῖας ἑαυτοῖς ἀνθομολογήσασθαι διότι προσέχουσι. καθαιρεθέντων δὲ τούτων λοιπὸν (ὁ) σημαίων ἀρεῖ μὲν τοὺς πρώτους ἐκ τῶν εὐωνύμων, διασαφῶν τὸ πλατεῖον ποῖον δεήσει σκοπεῖν, οἷον ἐὰν μὲν τὸ πρῶτον, ἔν', ἂν δὲ τὸ δεύτερον, δύο, καὶ [12] κατὰ λόγον οὕτω· τοὺς δὲ δευτέρους ἐκ τῶν δεξιῶν κατὰ τὸν αὐτὸν λόγον, ποῖον δεήσει γράμμα τῶν ἐκ τοῦ πλατείου γράφειν αὖ τὸν ἀποδεχόμενον τὴν πυρσεῖαν.

#### Prima di tradurre

- Lavorate alla consueta analisi dei verbi e delle proposizioni. Vista la complessità di alcuni periodi, potrebbe essere utile ricorrere alla schematizzazione.
- Prestate attenzione alle concordanze tra le parole.
- Ripassate i significati e la costruzione del verbo δέω/δέομαι.

#### Guida alla traduzione

- διασαφεῖν (riga 2): da che cosa è retto questo infinito?
- δεῖ (riga 3): con che cosa è costruito? Come si traduce quindi?

- δεῖ (riga 4): con che cosa è costruito? Come si traduce in quest'altro caso?
- λαμβάνοντας (riga 4): che valore ha questo participio? Qual è la sua funzione logica?
- λείπει (riga 4): attenzione al significato di questo verbo: qui è usato in uno dei suoi significati intransitivi. Che parola regge?
- παρεσκευάσθαι (riga 5): quale verbo sottinteso regge questo infinito? Fate riferimento al periodo precedente.
- τοὺς μέλλοντας (riga 5): che valore ha questo participio? Qual è la sua funzione logica nella frase? Quale altra voce verbale regge?

## 2. Svetonio, *Vita di Cesare*, 56 e *Vita di Augusto*, 88:

Nelle *Vite dei Cesari* Svetonio fornisce una testimonianza dell'utilizzo di codici segreti da parte di Cesare e di Augusto: si tratta di una delle pochissime fonti che parlano di crittografia vera e propria nel mondo romano. Il meccanismo alla base di entrambi i codici è molto semplice e la sua invenzione è attribuita da Svetonio a Cesare stesso, mentre Augusto lo adottò introducendo qualche piccola variante. Il codice di Cesare rimase celebre attraverso i secoli, anche se la sua decrittazione non presenta particolari difficoltà; un metodo efficace per decifrare questo e altri cifrari più complicati ma costruiti in base allo stesso criterio fu escogitato dal filosofo e matematico arabo Al-Kindi, vissuto nel IX secolo.

### 2.1. Svetonio, *Vita di Cesare*, 56:

Sono nominate in questo passo alcune lettere scritte in codice che Cesare mandava a Quinto Tullio Cicerone, suo luogotenente e fratello dell'oratore, e ai propri familiari.

*[...] Exstant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si quis inuestigare et persequi volet, quartam elementorum litteram, id est D pro A et perinde reliquas commutat.*

### 2.2. Svetonio, *Vita di Augusto*, 88:

In questo passo si parla in generale del rapporto di Augusto con l'ortografia (!); a queste notizie Svetonio aggiunge il riferimento al codice segreto usato dall'imperatore in alcune lettere.

*Orthographiam, id est formulam rationemque scribendi a grammaticis institutam, non adeo custodit ac videtur eorum potius sequi opinionem, qui perinde scribendum ac loquamur existiment. Nam quod saepe non litteras modo sed syllabas aut permutat aut praeterit, communis hominum error est. Nec ego id notare, nisi mihi mirum videretur tradidisse aliquos, legato eum consulari successorem dedisse ut rudi et indocto, cuius manu "ixi" pro "ipsi" scriptum animaduerterit. Quotiens autem per notas scribit, B pro A, C pro B ac deinceps eadem ratione sequentis litteras ponit; pro X autem duplex A.*

#### Prima di tradurre

- Ripassate la costruzione del periodo ipotetico e i pronomi indefiniti;
- Analizzate entrambi i testi come di consueto. I periodi non sono lunghi, ma sono piuttosto complessi, con molte subordinate.

## Guida alla traduzione

*N.B. le righe sono contate considerando i due brani come un unico testo.*

- *qua* (riga 1), *quis* (riga 2): che parte del discorso sono? Perché si trovano in questa forma?
- *existiment* (riga 5): giustificate questo congiuntivo.
- *notarem... nisi videretur* (righe 6-7): giustificate entrambi i congiuntivi.
- *ut* (riga 7): che funzione ha qui *ut*? È congiunzione subordinante?

## 3. Confronto, interpretazione e rielaborazione personale

1. Sulla base delle indicazioni riportate dai due autori:
  - a. disegnatte la “scacchiera di Polibio”: tenete presente che Polibio l’ha descritta pensando all’alfabeto greco. Provate ad adattarla all’alfabeto latino.
  - b. decifrate il titolo di questa dispensa; scoprite con quale dei due codici segreti descritti da Svetonio è stato cifrato. Potete procedere per tentativi oppure adottare il metodo dell’analisi delle frequenze di Al-Kindi (trovate il link alla descrizione più avanti).
2. Le descrizioni dei codici in greco e in latino ruotano attorno a un termine-chiave nelle rispettive lingue: *λόγος* in greco, *ratio* in latino. Rintracciate queste parole nel testo. Quale delle loro traduzioni è la più adatta al contesto? Giustificate la vostra scelta ragionando sui significati di queste due parole, importantissime per il lessico filosofico, matematico e scientifico delle due lingue. Individuate inoltre tutti gli altri termini tecnici della crittologia che compaiono nei testi proposti.
3. Polibio e Svetonio ci raccontano di due casi in cui una branca della matematica, la crittografia, entra in gioco nell’arte della guerra e nella diplomazia. Riflettete sul ruolo che le scienze e la tecnica potevano rivestire nell’arte militare greca e/o romana; motivate le vostre osservazioni. Citate inoltre, se potete, almeno un episodio della storia antica in cui una conoscenza scientifica abbia fornito un aiuto concreto in un contesto bellico.

## 4. Ulteriori letture

- ✓ La scelta dei brani è stata determinata dalla consultazione di questi due link, tratti dallo stesso sito, che è una vera e propria enciclopedia della crittologia: <http://www.crittologia.eu/critto/caes.htm> per i passi di Svetonio e <http://www.crittologia.eu/tele/polibio.html?chiaro=allahu%20akbar&OK=%20Codifica> per la descrizione tecnica della scacchiera di Polibio.
- ✓ A questo link trovate un’ulteriore e ancora più approfondita spiegazione della scacchiera di Polibio: <http://arjelle.altervista.org/Tesine/GiuliaG/polibio1.htm>
- ✓ Metodi rudimentali – in alcuni casi molto rudimentali – per proteggere messaggi importanti da sguardi indiscreti erano noti ai politici e ai capi militari fin dai tempi più antichi. Erodoto racconta del sistema escogitato per innescare la rivolta di Mileto, che fu il primo focolaio della rivolta delle città ioniche contro l’Impero persiano nel 499 a. C.: il messaggio che invitava alla ribellione la popolazione fu tatuato sul cranio rasato di un servo, al quale poi furono fatti ricrescere i capelli. Il passo delle *Storie* (V, 35) è disponibile in greco a questo link: <http://www.poesialatina.it/ns/Greek/testi/Herodotus/Historiae05.html>.
- ✓ Uno strumento per cifrare messaggi di ben altra complessità era la scytala, un bastone in dotazione alle spie degli Spartani, descritto da Plutarco nella *Vita di Lisandro*. Se volete sapere

come funzionava, traducete il paragrafo 19, 5 che trovate al seguente link:

<http://www.poesialatina.it/ns/Greek/testi/Plutarchus/Lysander.html>.

- ✓ Non alla matematica, ma alla chimica ricorrevano gli amanti romani che volevano mandarsi messaggi all'insaputa dei rispettivi coniugi: Ovidio nell'*Arte di amare* testimonia il frequente uso di inchiostri simpatici tra innamorati. Plinio il Vecchio ci descrive una pianta utile come ingrediente per la ricetta di un inchiostro invisibile al paragrafo XXVI, 39 della *Storia naturale*:  
<http://www.poesialatina.it/ns/ProsaLat/PlinSen/NH26.html>.
- ✓ A questo link trovate infine la descrizione del metodo dell'analisi delle frequenze di Al-Kindi, utile per decifrare i codici a sostituzione monoalfabetica come il codice di Cesare:  
<http://annalisasanti.blogspot.com/2016/11/al-kindi-e-hedy-lamarr-il-fascino-della.html>.