Al-Kindi, il padre della crittoanalisi

Abu Yūsuf Ya'qūb ibn 'Isḥāq aṣ-Ṣabbāḥ al-Kindī [nacque nell'801 a Basra, Iraq e morì a Bagdad nell'873] è conosciuto come «il filosofo degli arabi» ma fu anche un sapiente, un matematico, un medico, un musicista ed un crittologo. Fu il primo filosofo peripatetico arabo ed è ancora comunemente considerato come il padre della filosofia araba per la sua sintesi, il suo adattamento e la sua promozione della filosofia greca classica ed ellenistica nel mondo musulmano.
In questa sede analizziamo il suo contributo alla crittologia.
Consideriamo, a scopo di esempio, la cifra monoalfabetica [cioè che ha un solo alfabeto cifrante] ebraica nota come Atbash. In essa abbiamo un alfabeto chiaro [in verde nella tabella] ed un alfabeto cifrante [in rosso nella tabella].

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
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

Per cifrare il messaggio: «crittografia classica», prendiamo una lettera alla volta del messaggio chiaro, dalla prima all'ultima e la cerchiamo nell'alfabeto chiaro [verde]. Una volta che l'abbiamo trovata scendiamo nella riga inferiore della tabella e prendiamo la lettera della casella corrispondente. La successione di tali lettere costituisce il messaggio cifrato o cifra.
In questo esempio la prima lettera del messaggio, la c, viene cifrata con la X, la seconda lettera, r, viene cifrata con la I e così fino alla fine del messaggio chiaro, la cui cifra è: XIRGGLTIZURZ XOZHHRXZ .

Il destinatario del messaggio cifrato, procedendo in modo simmetrico alla cifratura, riesce a ricavare il messaggio chiaro. [Si cercano nell'alfabeto cifrante, una per volta, le lettere del messaggio cifrato. Trovatele si risale alla lettera nella casella immediatamente superiore dell'alfabeto chiaro. La successione delle lettere in chiaro così ottenute costituisce il messaggio comprensibile]. Tale procedura prende il nome di decifrazione.
Ma se un terzo personaggio, diverso dal mittente e dal destinatario, venisse in possesso del messaggio cifrato e non conoscesse l'alfabeto cifrante potrebbe comunque «leggerlo in chiaro?»
La risposta è: «Sì! Grazie al contributo di Al-Kindi».
Ipotizzando che la lingua in cui è stato scritto il messaggio sia l'italiano e che la distribuzione delle frequenze delle lettere del messaggio sia simile a quella della lingua italiana, allora prendiamo un vocabolario della lingua italiana e scegliamo tutte le parole con esclusione della loro definizione allo scopo di calcolare queste frequenze. Quindi contiamo tutte le a presenti in queste parole del vocabolario, poi tutte le b, poi tutte le altre lettere a seguire. Quindi dividiamo tutti questi valori per il numero totale delle lettere [moltiplicato per cento] ed otteniamo così la frequenza percentuale di ogni lettera. La e è la lettera più frequente: la sua frequenza corrisponde circa al 10% del totale, la a all'8%, la i al 9% e così a seguire.

[Nota. Le lettere accentate o con altri segni diacritici vanno sostituite con le lettere del'alfabeto di base: cioè la lettera è = e, ê = e, ç = c, ecc.].
Adesso passiamo al cifrato: in esso calcoliamo la frequenza percentuale di ogni lettera. Poi paragoniamo le frequenze del messaggio cifrato e della lingua italiana: ad una data frequenza di una lettera del messaggio cifrato, potrebbe corrispondere un'analoga o simile frequenza di un'altra lettera della lingua italiana, possiamo allora porre una relazione di corrispondenza tra le due lettere, cioè una lettera è la cifra dell'altra. Esempio: se la lettera del messaggio cifrato K ha una frequenza nel cifrato pari al 10% circa, probabilmente la K del messaggio cifrato corrisponde alla e del messaggio chiaro [anch'essa ha una frequenza del 10% circa]. Così, con pochi tentativi, si riesce a risolvere il messaggio cifrato. Il metodo dell'analisi delle frequenze è stato il contributo di Al-Kindi alla crittologia: questa tecnica ha costituito il primum movens della crittoanalisi, una branca della crittologia.
E vediamo la crittoanalisi in funzione… La regina di Scozia Maria Stuarda, cattolica, complotta con il cattolico Lord Babington contro sua cugina Elisabetta I, protestante, che la tiene prigioniera nella torre di Londra ma non ha alcuna intenzione di sopprimerla. Tra Maria Stuarda e Lord Babington intercorre un fitto scambio di messaggi che vengono intercettati dal controspionaggio di Elisabetta. Un uomo dei servizi segreti di Elisabetta, Felipes, a conoscenza della crittoanalisi di Al-Kindi, risolve tutti i messaggi cifrati con la cifra monoalfabetica dei congiurati. Questi messaggi dimostrano in modo incontrovertibile la partecipazione di Maria Stuarda alla congiura per assassinare la regina Elisabetta e per questo viene processata e condannata a morte mediante decapitazione che avverrà l'8 febbraio 1587.
Da questo episodio storico si evince come la cifratura monoalfabetica non sia affatto sicura.
La risposta dei crittografi all'analisi delle frequenze fu il ricorso alla cifratura polialfabetica che provocò un'analoga contro risposta crittoanalitica e questa guerra di tecniche e di ingegni continua ancor oggi!

Silvio dr Coccaro, medico – chirurgo, ex allievo 1972-1973