La crittografia nell'opera di Francis Bacon

Baron of Verulam, Viscount of St. Alban, Lord High Chancellor of England
A cura di Silvio Coccaro – Medico Chirurgo – Ex allievo 1972 – '73

Ad ciphras igitur veniendum. Earum genera haud pauca sunt: ciphrae simplices; ciphrae non significantibus characteribus intermixtae; ciphrae duplices literas uno charactere complexae; ciphrae rotae; ciphrae clavis; ciphrae verborum; aliae.
Primo, universae literae alphabeti in duas tantummodo literas solvantur per transpositionem earum. Nam transposition duarum literarum per locos quinque differentiis triginta duabus, multo magis viginti quatuor (qui est numerus alphabeti apud nos) sufficiet.

In poche righe, Bacone introduce il suo sistema cifrante basato su due lettere: a e b, opportunamente combinate in gruppi di cinque, secondo gli alfabeti seguenti:

Exemplum Alphabeti Biliterarii.					
A.	B.	C.	D.	E.	F.
aaaaa.	aaaab.	aaaba.	aaabb.	aabaa.	aabab.
G.	H.	I.	K.	L.	M.
aabba.	aabbb.	abaaa.	abaab.	ababa.	ababb.
N.	O.	P.	Q.	R.	S.
abbaa.	abbab.	abbba.	abbbb.	baaaa.	baaab.
T.	U.	W.	X.	Y.	Z.
baaba.	baabb.	babaa.	babab.	babba.	babbb.

In questo caso, per cifrare si ricorre al metodo della sostituzione dove ad ogni lettera del messaggio chiaro si sostituisce il gruppo di cinque lettere dell'alfabeto cifrante ad essa corrispondente. Da notare, però, che ciò ha lo svantaggio di aumentare di un fattore cinque la lunghezza del messaggio cifrato a cui, tra l'altro, si richiede:
Virtutes autem in ciphris requirendae tres sunt: ut sint expeditae, non nimis operosae ad scribendum: ut sint fidae, et nullo modo pateant ad deciphrandum: addo denique, ut, si fieri possit, suspicione vacent. Si enim epistolae in manus eorum devenient, qui in eos, qui scribunt, aut ad quos scribuntur, potestatem habeant, tametsi ciphra ipsa fida fit et deciphratu impossibilis, tamen subjicitur haec res examini et quaestioni; nisi ciphra sit ejusmodi, quae aut suspicione vacet, aut examinationem eludat.

Così, il messaggio chiaro viene cifrato nel messaggio intermedio, avendosi sostituito ogni suo carattere col gruppo di cinque lettere ad esso corrispondente: ad es., se il messaggio comincia con la parola Londinium, allora la sua prima lettera, la L, verrà sostituita con: **ababa** e così, analogamente, fino alla fine del messaggio chiaro.

Completata la cifratura del messaggio chiaro nel messaggio intermedio si procede al suo occultamento in un messaggio chiaro anodino con un'operazione di steganografia, cioè di dissimulazione nel messaggio apparentemente normale. Alla lettera a si associa un tipo di carattere, alla lettera b un tipo diverso. Con questi due tipi si scrive il messaggio anodino rispettando la cifratura intermedia. Es.: se la lettera da cifrare è la L, la cui cifra è

ababa e la a viene rappresentata col tipo di carattere normale e la b col tipo di carattere corsivo allora la successione dei tipi di caratteri: nomale, corsivo, normale, corsivo, normale occulta la L in «P*rimo*», se il messaggio anodino è «Primo».

Exemplum Alphabeti Biformis.

a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*
A.	*A.*	a.	*a.*	B.	*B.*	b.	*b.*	C.	*C.*	c.	*c.*	D.	*D.*	d.	*d.*	E.	*E.*
a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*
e.	*e.*	F.	*F.*	f.	*f.*	G.	*G.*	g.	*g.*	H.	*H.*	h.	*h.*	I.	*I.*	i.	*i.*
a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*
K.	*K.*	k.	*k.*	L.	*L.*	l.	*l.*	M.	*M.*	m.	*m.*	N.	*N.*	n.	*n.*	O.	*O.*
a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*
o.	*o.*	P.	*P.*	p.	*p.*	Q.	*Q.*	q.	*q.*	R.	*R.*	r.	*r.*	S.	*S.*	s.	*s.*
a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*	a.	*b.*
T.	*T.*	t.	*t.*	U.	*U.*	u.	*u.*	W.	*W.*	w.	*w.*	X.	*X.*	x.	*x.*	Y.	*Y.*
a.	*b.*	a.	*b.*	a.	*b.*												
y.	*y.*	Z.	*Z.*	z.	*z.*												

Epistola Interior.
Perditae res: Mindarus cecidit: milites esuriunt: neque hinc nos extricare, neque hic diutius manere possumus.

Epistola Exterior [da Cicerone].
Ego omni officio, ac potius pietate erga te, caeteris satisfacio omnibus: mihi ipse nunquam satisfacio. Tanta est enim magnitudo tuorum erga me meritorum, ut quoniam tu, nisi perfecta re, de me non conquiesti: ego, quia non idem in tua causa efficio, vitam mihi esse acerbam putem. In causa haec sunt: Ammonius regis legatus aperte pecunia nos oppugnat. Res agitur per eosdem creditores, per quos, cum tu aderas, agebatur. Regis causa, si qui sunt, qui velint, qui pauci sunt, omnes ad Pompeium rem deferri volunt. Senatus religionis calumniam, non religione, sed malevolentia, et illius regiae largitionis invidia comprobat, etc.

A questo punto, il lettore è invitato, come esercizio, a cifrare il messaggio su esposto [Epistola Interior], calcolando prima la cifra intermedia e poi occultandola nel messaggio non sospetto di Cicerone, secondo il metodo appena illustrato.

Questa cifra è originale e particolare per la sua epoca in quanto ricorre contemporaneamente alla crittografia ed alla steganografia, due branche distinte della crittologia.

Considerazioni finali sulla sua attualità. Essa si basa su due simboli soltanto, organizzati in quintetti, per poter rappresentare entità più complesse [il suo alfabeto cifrante di 24 lettere distinte], il che ha anticipato in un certo qual modo:

- l'alfabeto Morse, basato anch'esso su due simboli: il punto e la linea, raggruppati variamente, codice che è stato il fulcro delle prime comunicazioni via radio;
- il codice Baudot a due simboli [un foro sul nastro e la sua mancanza] raggruppati in quintetti, usato per gran parte del secolo scorso nelle telecomunicazioni mediante le telescriventi, cifranti e non;
- il sistema di numerazione binario [i bit 0 ed 1, raggruppati in ottetti, formano i byte, che costituiscono l'essenza dei computer moderni e delle loro tabelle ASCII ed ANSI].