

CRYPTOGRAPHIE ANTIQUE

1. Énée le Tacticien (IV^e s. av. J.-C.)

Γράφειν δὲ καὶ ὧδε. Προσυνθέμενον τὰ φωνήεντα γράμματα ἐν κεντήμασι τίθεσθαι, ὅποσον δ' ἂν τύχη ἕκαστον ὄν, ἐν τοῖς γραφομένοις τοσαύτας στιγμὰς εἶναι. Οἷον τόδε.

Διονύσιος καλός

Δ:::N::Σ:::ΣΚ·Λ::Σ·

[...] καὶ τόδε ἄλλο· ἀντὶ τῶν φωνηέντων γραμμάτων τίθεσθαι τί δαί.

« Mais on peut encore écrire ainsi : après s'être entendu avec le destinataire, remplacer les voyelles par des points et au rang que chacune d'elles occupe, placer dans les écrits des points aussi nombreux. Par exemple :

Denys est honnête.

D:N::S :ST H::NN:T:

[...] Et autre système : à la place des voyelles mettre un signe quelconque. »

voyelles	A	E	I	O	U	Y
code	.	:	∴	::	∴:	:::

2. Le code de Jules César (I^{er} s. av. J.-C.)

Exant 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 uerbum effici posset : quae si qui inuestigare et persequi uelit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet.

Suétone, *Vie de César*, LVI, 8

« Il existe ses lettres à Cicéron, de même que celles qu'il adressait à ses familiers sur ses affaires domestiques ; dans celles-ci, s'il devait leur faire quelques communications plus secrètes, il écrivait grâce à des codes, c'est-à-dire qu'il brouillait la succession des lettres de telle façon qu'aucun mot ne pût être reconstitué : si quelqu'un veut en découvrir le sens et les déchiffrer, il remplace chaque lettre par la quatrième qui suit dans l'alphabet, c'est-à-dire le D au lieu de l'A, et il change ensuite le reste. »

Alphabet clair	a	b	c	d	e	f	g	h	i/j	k	l	m	n	o	p	q	r	s	t	u/v	x	y	z
Alphabet chiffré	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	V

Texte clair : ueni, uidi, uici.

Texte chiffré : RBKF, RFAF, RFZF.

3. Le grec

Jules César commente au livre V du *De bello Gallico* le siège du quartier d'hiver de Q. Cicéron par les Nerviens. Encerclé, le légat tente de faire parvenir à César des messages implorant de l'aide : sans succès, tous les messagers sont capturés puis torturés par les ennemis. Finalement, Vertico, un Nervien, homme de confiance de Cicéron, convainc son esclave gaulois de se rendre au camp du général : cet esclave traverse les positions des assiégeants sans éveiller le moindre soupçon. Tenu au courant de la situation critique dans laquelle se trouve la légion, César se met en marche après avoir rassemblé ses troupes. Arrivé près du camp, il apprend de la bouche des prisonniers dans quel état se trouvent les troupes : il décide d'envoyer un message à Cicéron pour lui annoncer sa venue afin que lui et sa légion ne désespèrent pas et surtout afin qu'ils ne se rendent pas : un autre Gaulois proche de Vertico fait office de messenger.

Tum cuidam ex equitibus Gallis magnis praemiis persuadet uti ad Ciceronem epistolam deferat. Hanc Graecis conscriptam litteris mittit, ne intercepta epistola nostra ab hostibus consilia cognoscantur.

César, *Gaules*, V, XLVIII, 3-4

« Il persuade alors un cavalier gaulois, en lui promettant de grandes récompenses, de porter une lettre à Cicéron. Il envoie celle-ci écrite en **lettres grecques**, afin que, si elle est interceptée, nos desseins ne soient pas pénétrés par les ennemis. »

Alphabet grec

grec	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ/ς	τ	υ	φ	χ	ψ	ω	·
valeur phonétique	a	b	g	d	é	z	è	th	i	k	l	m	n	x	o	p	r	s	t	u	f	ch/kh	ps	ô	h aspiré

Comme les sons du français et du grec ne sont pas identiques, il faut employer des subterfuges :

- la lettre *c* pourra être transcrite soit κ (devant *a, o, u*, son [k]) soit σ (devant *e, i*, son [s]) ;
- la lettre *j* (ou *g* devant *e, i*, son [ʒ]) pourra être transcrite ι, voire ζ (variante zozotante) ;
- la lettre *e* pourra être transcrite ε, même lorsqu'elle se prononce [ø], comme dans *le*.
- les lettres *qu* pourront être transcrites κ, à la rigueur κυ ;
- la lettre *v* pourra se transcrire β, φ, ou, qui sont les sons les plus proches, ou bien ω qui ressemble à un *w* ;
- la lettre *w* sera transcrite ou pour le son [w], ou bien comme ν ;
- le *s* intervocalique pourra être transcrit ζ ;
- le *y* sera transcrit ι ;
- le son [u] sera transcrit ou ;
- le son *gn* [ɲ] pourra être transcrit γν ou νι ;
- les nasales *in/ain/ein, en/an, on* (et leurs variantes en *-m*) pourront être translittérées ou transcrites phonétiquement ιν/εν/ον ;
- dans tous les cas, on pourra choisir une translittération aussi stricte que possible, ou une transcription phonétique, ou un mélange des deux :
 - o *eau* pourra ainsi s'écrire εαυ ou ω
 - o *problème* pourra s'écrire προβλημε ou προβλημ
 - o *inventaire* pourra s'écrire ινφεντηρ, ινωεντηρ, ινβενταιρ, ...
 - o *empreinte* pourra s'écrire εμπρειντε, εμπριντε, εμπριντ, ενπριντ, ...

Exemple 1 : Κανδ ον τε διτ « βεαυκουπ δε σεριζες », πρενδς υν πετιτ πανιερ.

Quand on te dit « beaucoup de cerises, prends un petit panier. (proverbe grec)

Exemple 2 : Σευλ τον ονγλ ση ου τε γρατε.

Seul ton ongle sait où te gratter.

Variante : coder l'alphabet grec en utilisant le code de César

nom des lettres	alpha	bêta	gamma	delta	epsilon	dzêta	êta	thêta	iota	kappa	lambda	mu	nu	xi	omicron	pi	rho	sigma	tau	upsilon	phi	chi	psi	oméga
alphabet clair	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ	ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω
alphabet chiffré	X	Ψ	Ω	A	B	Γ	Δ	E	Z	H	Θ	I	K	Λ	M	N	Ξ	O	Π	P	Σ	T	Υ	Φ

Exemple : Σχψξζηγκμ σζπ σχψδξ.

FABRICANDO FIT FABER

4. Le carré de Polybe ou le carré de 25.

Ἔστι δὲ τοιοῦτος. Τὸ τῶν στοιχείων πλῆθος ἐξῆς δεῖ λαμβάνοντας διελεῖν εἰς πέντε μέρη κατὰ πέντε γράμματα. Λείψει δὲ τὸ τελευταῖον ἐνὶ στοιχείῳ· τοῦτο δ' οὐ βλάπτει πρὸς τὴν χρείαν.

On doit prendre dans l'ordre l'ensemble des lettres de l'alphabet et les diviser en cinq groupes de cinq lettres. Il manquera au dernier une lettre ; mais ce n'est pas gênant pour l'opération. (Polybe X, XLV, 7)

Selon ces données, le carré de Polybe se présente ainsi :

	1	2	3	4	5
1	a	f	l	q	w
2	b	g	m	r	x
3	c	h	n	s	y
4	d	i/j	o	t	z
5	e	k	p	u/v	

Τούτων δ' ἐτοιμασθέντων παρ' ἀμφοτέροις, ὅταν βούλῃ δηλῶσαι λόγου χάριν διότι “τῶν στρατιωτῶν τινες εἰς ἑκατὸν ἀποκεχωρήκασιν πρὸς τοὺς ὑπεναντίους,” πρῶτον δεῖ διαλέξαι τῶν λέξεων, ὅσαι δι' ἐλαχίστων γραμμάτων δύνανται ταῦτ' ἀποδοῦναι, οἷον ἀντὶ τοῦ προειρημένου “Κρήτες ἑκατὸν ἀφ' ἡμῶν ἡτομόλησαν.” Νῦν γὰρ τὰ μὲν γράμματα' ἐστὶν ἐλάττω τῶν ἡμίσεων, διασφαεῖται δὲ ταῦτόν. Τούτου δὲ γραφέντος εἰς πινάκιον, οὕτω δηλωθήσεται τοῖς πυρσοῖς. Πρῶτον δ' ἐστὶ γράμμα τὸ κάππα· τοῦτο δ' ἐστὶν ἐν τῇ δευτέρᾳ μερίδι καὶ τῷ δευτέρῳ πλατεῖ. Δεῖσει δὲ καὶ πυρσοὺς ἐκ τῶν εὐωνύμων δὴ αἶρειν, ὥστε τὸν ἀποδεχόμενον γινώσκειν ὅτι δεῖ τὸ δεύτερον πλατεῖον ἐπισκοπεῖν. Εἴτ' ἐκ τῶν δεξιῶν ἀρεῖ πέντε, διασφαῶν ὅτι κάππα· τοῦτο γὰρ πέμπτον ἐστὶ τῆς δευτέρας μερίδος, ὃ δεῖσει γράφειν εἰς τὸ πινάκιον τὸν ἀποδεχόμενον τοὺς πυρσοὺς. (εἴτα τέτταρας ἐκ τῶν εὐωνύμων, ἐπεὶ) τὸ ῥῶ τῆς τετάρτης ἐστὶ μερίδος. Εἴτα δύο πάλιν ἐκ τῶν δεξιῶν· δεύτερον (γάρ) ἐστὶ τῆς τετάρτης. ἐξ οὗ τὸ ῥῶ γράφει [ὃ δεχόμενος τοὺς πυρσοὺς]· καὶ τὰ λοιπὰ τὸν αὐτὸν τρόπον.

« Une fois ces préparatifs achevés de part et d'autre, lorsqu'on veut signifier, par exemple : 'certains de nos soldats, cent environ, sont passés du côté de l'adversaire', on doit d'abord faire un choix des termes qui peuvent signifier la même chose avec très peu de lettres, comme par exemple, au lieu de ce qui a été dit précédemment : 'cent Crétois ont déserté notre camp'. À présent les lettres sont moitié moins nombreuses, mais elles font savoir la même chose. Ce texte (...) sera alors *chiffré*. La première lettre est *c* : elle se trouve sur la *troisième ligne* et dans la *première colonne*. On devra *inscrire 1* sur la gauche, de sorte que celui qui reçoit le message sache qu'il doit regarder la *première colonne*. Puis on devra *inscrire 3* sur la droite, ce qui veut dire *c*, car c'est la *troisième lettre de la première colonne*, et celui qui reçoit le message devra l'écrire sur la tablette. Ensuite *1* sur la gauche, puisque le *e* appartient à la *première colonne*, et à l'inverse *5* sur la droite, car c'est la *cinquième lettre du premier groupe*. Alors, celui qui reçoit le message écrit *e* ; et ainsi du reste. »

(d'après Polybe, X, XLVI, 4-10)

En appliquant cet exemple au tableau ci-dessus, nous obtenons :

lettre	colonne	ligne	chiffre
c	1	3	13
e	1	5	15

Exemple : 43 24 45 24 43 35 11 13 15 32, 35 11 42 11 12 15 31 31 45 32.

SI VIS PACEM, PARA BELLUM

Variante 1 : utiliser le carré de Polybe avec l'alphabet grec

Cf. p. 2 pour la transcription du français au grec.

Exemple : 54 24 54 15 31 15 43 54 11 25 11 33 43.

ωιωε λες ωακανς : vive les vacances

	1	2	3	4	5
1	α	ζ	λ	π	φ
2	β	η	μ	ρ	χ
3	γ	θ	ν	σ/ς	ψ
4	δ	ι	ξ	τ	ω
5	ε	κ	ο	υ	

Variante 2 : utiliser le carré de Polybe avec l'alphabet grec ET les chiffres grecs !

L'exemple précédent devient alors :

εδ'βδ'εδ'αε' γα'αε'δγ' εδ'αα'βε'αα'γγ'δγ'

	α'	β'	γ'	δ'	ε'
α'	α	ζ	λ	π	φ
β'	β	η	μ	ρ	χ
γ'	γ	θ	ν	σ	ψ
δ'	δ	ι	ξ	τ	ω
ε'	ε	κ	ο	υ	

5. La scytale

Mode d'emploi de la scytale lacédémonienne (spartiate) chez Aulu-Gelle (*Nuits attiques*, XVII, 9, 6-14).

Lacedaemonii autem ueteres, cum dissimulare et occultare litteras publice ad imperatores suos missas uolebant, ne, si ab hostibus eae captae forent, consilia sua noscerentur, epistulas id genus factas mittebant. Surculi duo erant teretes, oblonguli, pari crassamento eiusdemque longitudinis, derasi atque ornati consimiliter; unus imperatori in bellum proficiscenti dabatur, alterum domi magistratus cum iure atque cum signo habebant. Quando usus uenerat litterarum secretiorum, circum eum surculum lorum modicae tenuitatis, longum autem, quantum rei satis erat, conplicabant uolumine rotundo et simplici, ita uti orae adiunctae undique et cohaerentes lori, quod plicabatur, coirent. Litteras deinde in eo loro per transversas iuncturarum oras uersibus a summo ad imum proficiscentibus inscribebant. Id lorum litteris ita perscriptis reuolutum ex surculo imperatori commenti istius conscio mittebant; resolutio autem lori litteras truncas atque mutilas reddebat membraque earum et apices in partis diuersissimas spargebat; propterea, si id lorum in manus hostium inciderat, nihil quicquam coniectari ex eo scripto quibat; sed ubi ille, ad quem erat missum, acceperat, surculo conpari, quem habebat, <a> capite ad finem, proinde ut debere fieri sciebat, circumplicabat, atque ita litterae per eundem ambitum surculi coalescentes rursum coibant integramque et incorruptam epistulam et facilem legi praestabant. Hoc genus epistulae Lacedaemonii σκυτάλην appellant.

Les anciens Lacédémoniens, quand ils voulaient dissimuler et cacher les lettres envoyées par le gouvernement à leurs généraux, afin que leurs projets ne fussent pas percés si les lettres tombaient aux mains de l'ennemi, envoyaient des lettres faites de la manière suivante. Deux longues baguettes cylindriques, de la même épaisseur et de la même longueur, avaient été écorcées et préparées de la même manière. L'une était donnée au général qui partait à la guerre, l'autre, les magistrats la gardaient à Sparte sous leur autorité et sous leur sceau. Quand on avait besoin de messages un peu secrets, ils enroulaient autour de cette baguette une lanière de cuir d'une épaisseur moyenne, mais de longueur nécessaire, en une spirale simple de telle sorte que les bords de la lanière qu'on enroulait fussent joints et solidaires. Ils inscrivaient ensuite le message sur cette lanière, en chevauchant les bords joints sur des lignes qui partaient du haut jusque en bas. Une fois la lettre écrite ainsi, ils déroulaient du bâton la lanière pour l'envoyer au général qui était au courant de cette invention. Or la lanière une fois détachée, les lettres devenaient morcelées et mutilées, morceaux et contours dispersés dans les directions les plus opposées ; c'est pourquoi si cette lanière tombait aux mains des ennemis, ils ne pouvaient rien tirer de cet écrit. Mais quand celui à qui le message était envoyé l'avait reçu, il l'enroulait du haut jusqu'en bas sur la baguette de même dimension qu'il détenait, comme il savait que cela devait être fait, et ainsi, les lettres se réunissant grâce à l'identité de la circonférence des baguettes, elles formaient un tout à nouveau et fournissaient le message entier, intégral et facile à lire. Ce genre de message, les Lacédémoniens l'appellent *skutalè*.

L'illisibilité du message déroulé sera d'autant plus grande que la bande est étroite. En effet, plus la bande sera étroite, plus elle accomplira un grand nombre de circuits autour du bâton, ce qui rendra le décryptage plus ardu. L'idéal serait que chaque circuit ne contienne qu'une seule lettre, comme le dit Aulu-Gelle afin d'éclater le message en des lettres isolées. Enfin, la superposition des lignes protégera mieux le message créant des difficultés de lecture plus profondes.

Variantes : utiliser tous les systèmes de chiffrement vus précédemment avant de copier le message sur la scytale.

