Codes secrets et Transmissions

CIRSSA de DOUAI

Directeur: PCP VANDEPUTTE Hervé.

La place du Service de Santé des Armées.

Novembre 2013

Pr. M-M.DEMINATTI

Le télégramme de Zimmermann

3 août 1914: Déclaration guerre: l' Allemagne à la France.

4 sept 1914: Déclaration de guerre: G-B à l'Allemagne.

5 sept 1914 au matin: câblier anglais *Telconia.* (B.T.p.17) : Emden.

Section de 5 câbles transatlantiques allemands: Brest, Vigo (Espagne), Ténériffe (Canaries), 2 New-York via Açores. (B.T.p.17).

Reste 1 câble Afrique occidentale – Brésil (Eastern Telegraph) (B.T.p.18).

Moyens de transmission Allemagne-USA (B.T.p.192-193).

- <u>aériens</u>: station radio: Nauen (près de Berlin). (Ambassade USA: Copenhague puis câble G-B.)

- <u>câblés</u> via la Suède. Transit par la GB. Télégramme Zimmermann (S.Singh:p.146)

- <u>humains</u>: employé Ambassade USA à Berlin câble diplomatique USA (B.T.p.193) .

Moyens d'interception britanniques

<u>Tous les câbles</u>

13 oct 1914: livre-code Marine allemande. ''Magdeburg'' (B.T.p.21-22) .

1915: livre-code diplomatique n°13040.(A.Szek) (W.Wassmuss) (B.T.p.26-31)

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.141-151.

Le secret de la Grande Guerre. Barbara Tuchman. Librairie Arthème Fayard, Paris, 1965.p.17,

Zimmermann (Berlin). 16 janv. 1917.

1 fév 1917: U-boot Krieg.

3 voies (B.T.p.193)

Von Bernstoff (Washington).

Version ''américaine''.
(B.T.p.192-193).

19 janv 1917.

Voie: *Western Union.*

5 fév 1917: Message d'intervention. Voie ''suédoise'' (B.T.p.200).

Version ''mexicaine''.

Code diplomatiquen°13040. n°5950.
code marine VB718 (B.T.p.103)

Le télégramme de Zimmermann

Von Eckardt (Mexico).

- Londres: Forme codée (10 fév) décodée (19 fév) (B.T.p.209)

Le casse-tête à Londres: avoir la version mexicaine décodée par von Eckardt (B.T.p.203-230) .

- 23 fév: Foreign Office: remise du télégramme à l'Ambassadeur USA (B.T.p.215)

- *Laconia (Cunard)* (26 fév), 3 navires marchands (18 mars) (B.T.p.224, 259).

Président du Mexique.

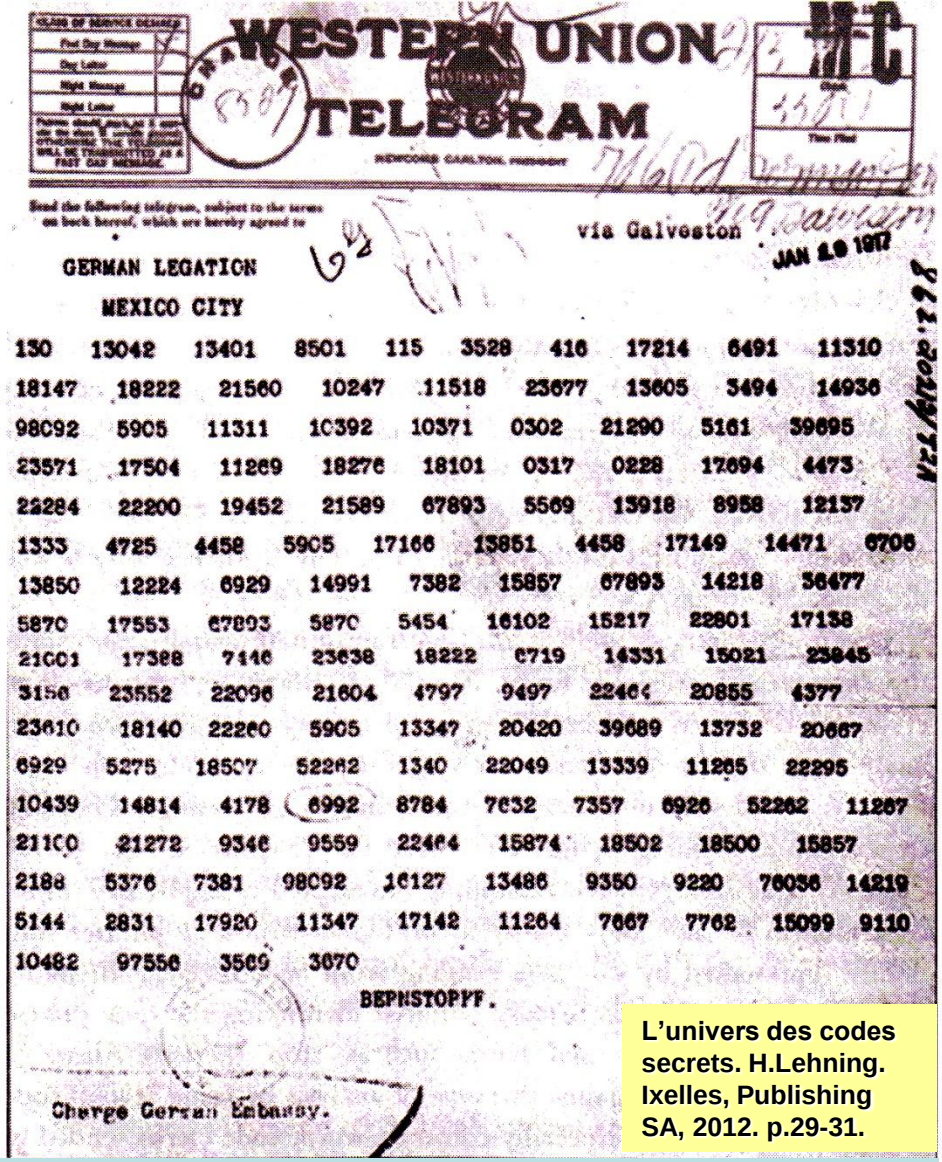
- 1 mars: *Times*. (B.T.p.228) .

- 3 mars: Zimmermann avoue la paternité du télégramme (B.T.p.238)

6 avril 1917: USA déclarent la guerre au IIème Reich.

Le secret de la Grande Guerre.
Barbara Tuchman. Librairie Arthème Fayard, Paris, 1965.

Le télégramme de Zimmermann



WESTERN UNION TELEGRAM

Read the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

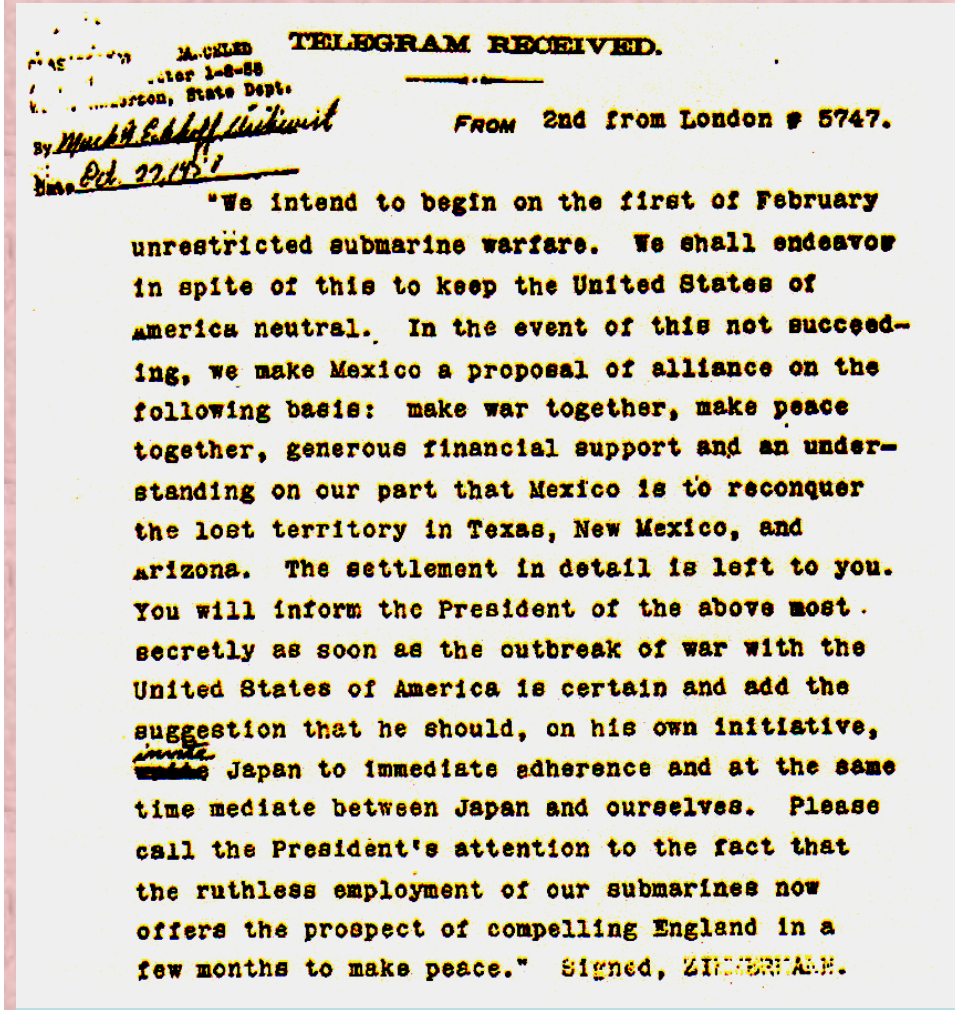
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7146 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTOPFF.

Charge German Embassy.

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.29-31.

Télégramme de Zimmermann



TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Version déchiffrée du télégramme.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. p.16-21.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.141-151.

Les composantes de l'Univers.

Physiques: lois physiques.

Chimiques: lois chimiques.

Biologiques: lois biologiques.

Relationnelles et Comportementales.

La gravitation: chute de la pomme.

Acide + Base: Sel (échange d'atomes, d'électrons).

Reproduction. Cerveau – cœur. Chat – souris.

EAU: H_2O.

Les trois dimensions: 3 D: hauteur, largeur, profondeur.

Le temps: chronologie, durée: 4ème Dimension.

Stress et génome. M-M. Deminatti. *in* : Vers une médecine de l'homme en mouvement. H. Périé *et al.* Éditions Frison-Roche. Paris. 2006. p. 239-259.

Couche matérielle:

"hardware"

Émetteurs, récepteurs.

Voix, gestes, écriture,… , télégraphe, téléphone, etc…

"le relationnel humain". La 5ème dimension: le cyberespace:

Structures de l'interconnexion: câbles (cuivre, optique), ondes, relais (terre, mer, espace).

Noosphère: "sphère pensante".

Couche logique, logicielle:

"software"

Codes, langages, protocoles, procédures.

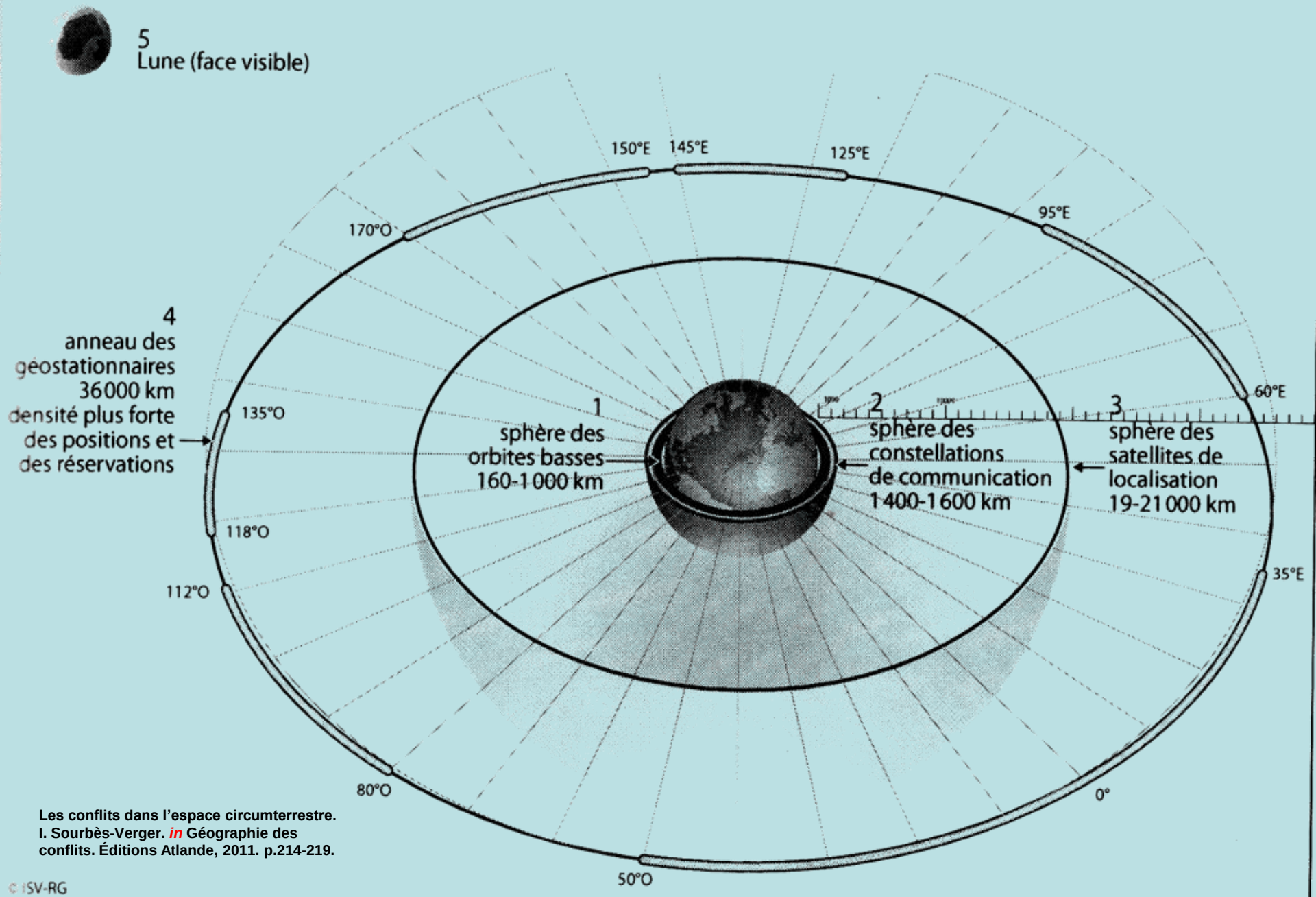
Couche sémantique et informationnelle:

Informations (créées, transportées, utilisées,…)

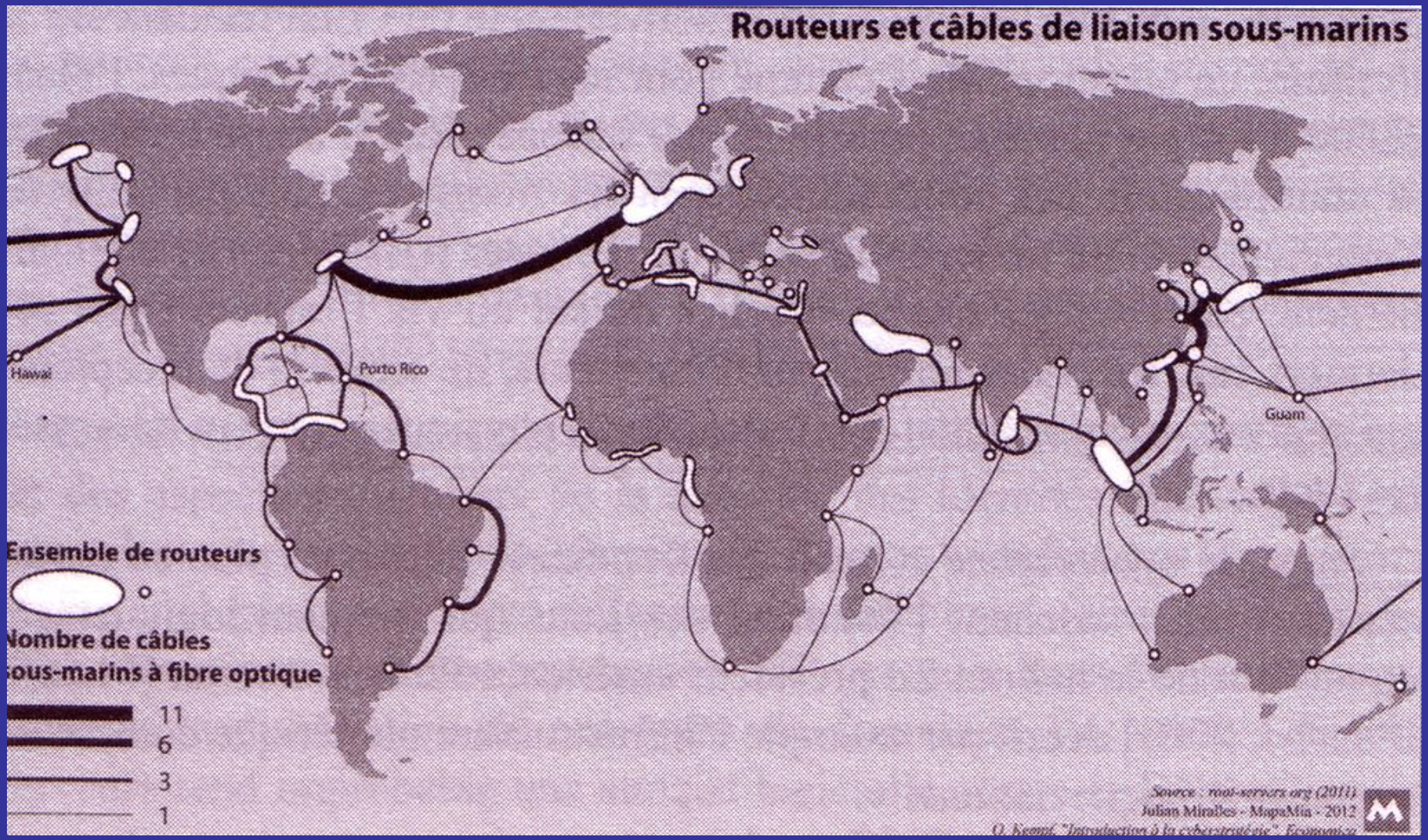
Individus, institutions, etc..

Introduction à la cyberstratégie. O. Kempf. Éditions Economica, Paris, 2012. p.10-14; p.40.

La place de l'homme dans la nature. P.Teilhard de Chardin. Éditions Albin Michel, Paris,1956. (p.111).



Les conflits dans l'espace circumterrestre. I. Sourbès-Verger. *in* Géographie des conflits. Éditions Atlande, 2011. p.214-219.



Introduction à la cyberstratégie. O. Kempf. Éditions Economica, Paris, 2012. p.21.

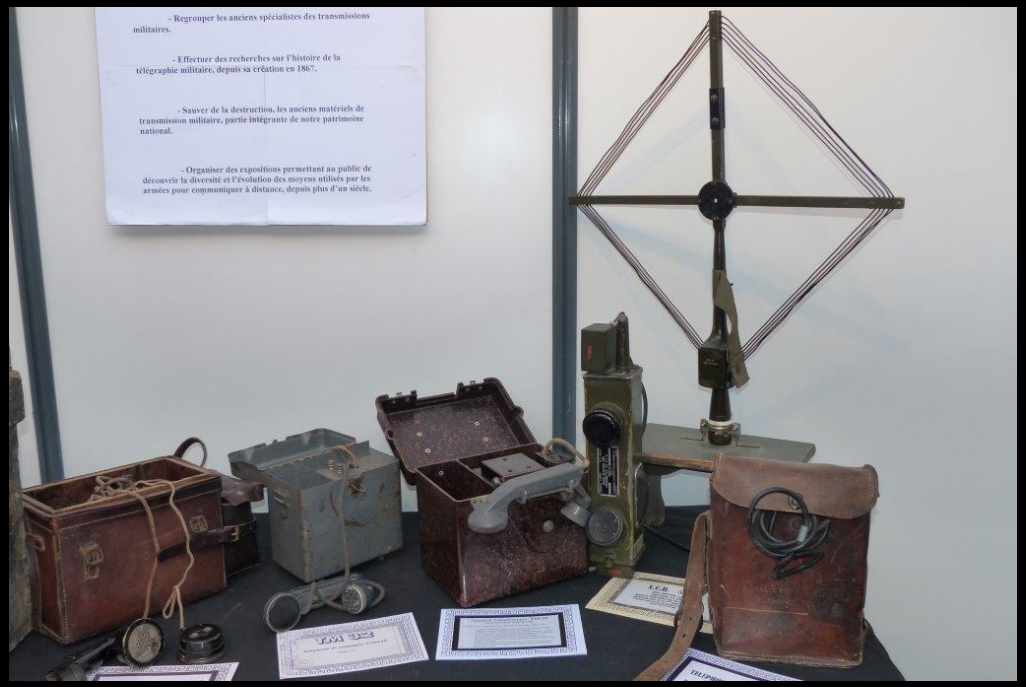
TRANSMISSIONS MILITAIRES
189
AMICALE DES TRANSMISSIONS
de la Côte d'Azur

Nice 2013.

Nice 2013.

Nice 2013.

- Organiser des expositions permettant au public de découvrir la diversité et l'évolution des moyens utilisés par les armées pour communiquer à distance, depuis plus d'un siècle.
CENTRAL TELEPHONIQUE D'ARTILLERIE Modèle 1918


- Regrouper les anciens spécialistes des transmissions militaires.
- Effectuer des recherches sur l'histoire de la télégraphie militaire, depuis sa création en 1867.
- Sauver de la destruction, les anciens matériels de transmission militaire, partie intégrante de notre patrimoine national.
- Organiser des expositions permettant au public de découvrir la diversité et l'évolution des moyens utilisés par les armées pour communiquer à distance, depuis plus d'un siècle.

Nice 2013.

Nice 2013.

Les transmissions sont au coeur de l’opération Serval

Centre d'écoute de la R.A.F. (Menwith Hill – Yorkshire: U.K.): cadre Echelon USA (NSA)- UK.

Prism : 2007 : USA (NAS): Internet.

Entreprises: échanges, stockage, chiffrement (clefs).

« tout le monde espionne tout le monde »

L'Europe à la merci de l'espionnage américain. J-P Stroobants, F Lemaître. Le Monde 12 juin 2013.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.382.

France: DGSE (Paris: Bd Mortier): ''cyber-écoute''.

Pensée

Parole

Écriture
(image, son,..)

Transcription

Émission

Message

Supports

Algorithme

Codes

Chiffres

Clefs

Milieux (aérien, liquide, solide) - distance – temps – confidentialité - ,,,

Réception

Traduction

Écriture
(image, son,..)

Parole

Pensée

“ l’arme qui unit les armes”
devise des Transmissions de l’Armée française.

La communication et sa confidentialité

ADN

Chaîne phosphatée.

Sucre: désoxyribose.

4 bases: adénine, guanine, thymine, cytosine.

atgcccatga gtcagttaccgtttattc attagca

Transcription.

Complémentarité: a–t (u RNAm), g-c.

Chaîne phosphatée.

Sucre: ribose.

4 bases: adénine, guanine, uracile, cytosine.

Messager: ARN.

cagucaauggcaaauaag

Traduction.

Code génétique: combinaisons de 3 bases: a, u, g, c: 4^3: 64 triplets.

caguc aau ggc aaa uaa g

caguca aug gca aau aag

20 acides aminés.

Milliers de protéines.

asparagine-alanine-lysine-STOP.

Méthionine-alanine-asparagine-lysine-….

La cryptologie.

Émetteur.

Récepteur.

Chiffrement.

Déchiffrement.

Algorithme + clef.

Cryptographie

Algorithme + clef.

Message chiffré.

Support du message.

Interception volontaire, involontaire du message.

Cryptanalyse

Écriture du message.

Stéganographie (couverte).

Cryptographie (cachée).

Transposition des phrases, mots, lettres.

Substitution.

Substitution + transposition

Chiffre (change les lettres).

Code (change les mots en autres mots, chiffres,…).

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris. p.53.

La stéganographie:
steganos=couvert;
graphos=écrire.

Dissimulation du message des supports,…

La cire: Démarate (484 avJC)

Le crâne rasé: Hitiée à son gendre tyran de Milet

L'encre sympathique: jus de citron, urines, jus d'euphorbe,…

Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.65.

Musset et George Sand.

Le micropoint de Zapp: photographie réduite à un point de 1 mm ou moins.

Etc…

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.20.

La stéganographie:

Un autre exemple de cryptographie familière était l'usage répandu du cryptage par piqûres d'épingle. L'historien de la Grèce antique Énée le Tacticien imagina d'envoyer un message secret en piquant de minuscules trous sous certaines lettres dans une page apparemment anodine, tout comme vous voyez des points sous certaines lettres de ce paragraphe.

LELIVREDESCODES

Deux mille ans plus tard, les épistoliers anglais employèrent la même méthode, non pour assurer le secret à leurs envois, mais pour éviter de payer des taxes postales excessives.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.112.

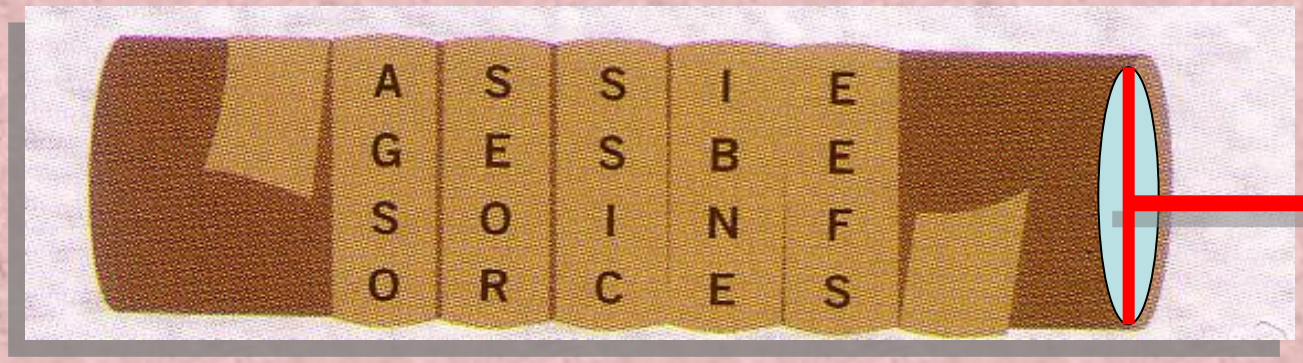
La cryptographie.

Le chiffrement par <u>transposition de lettres</u>

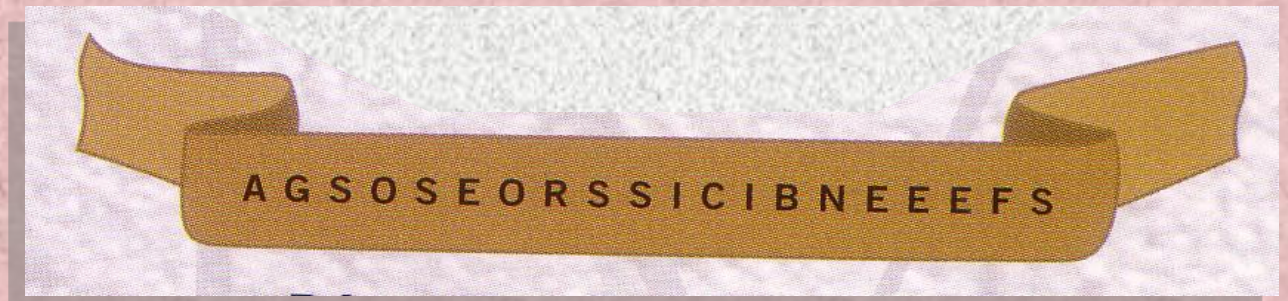
La scytale spartiate → **Algorithme**

« assiégés besoin forces »

Parchemin.



Clef



Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.102.

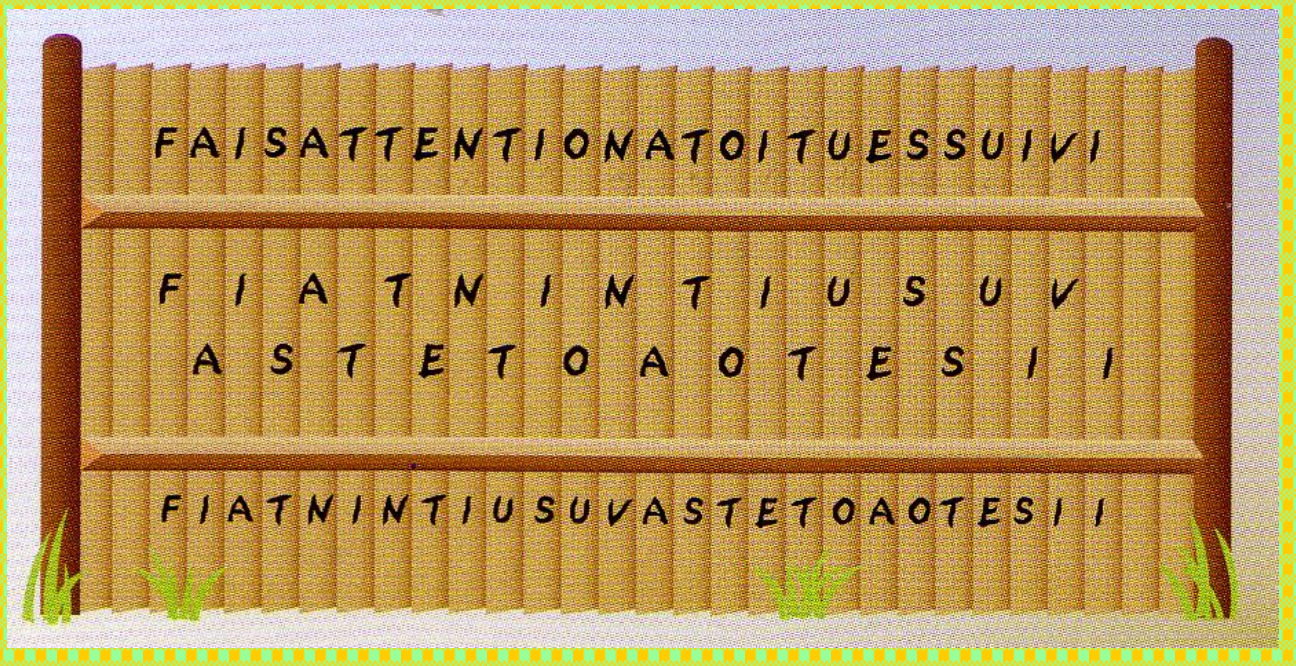
Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris. p.25.

La cryptographie.

Le chiffrement par <u>transposition de lettres</u>

Transposition dite ‘’en dents de scie” sur deux lignes:

« Fais attention à toi tu es suivi »



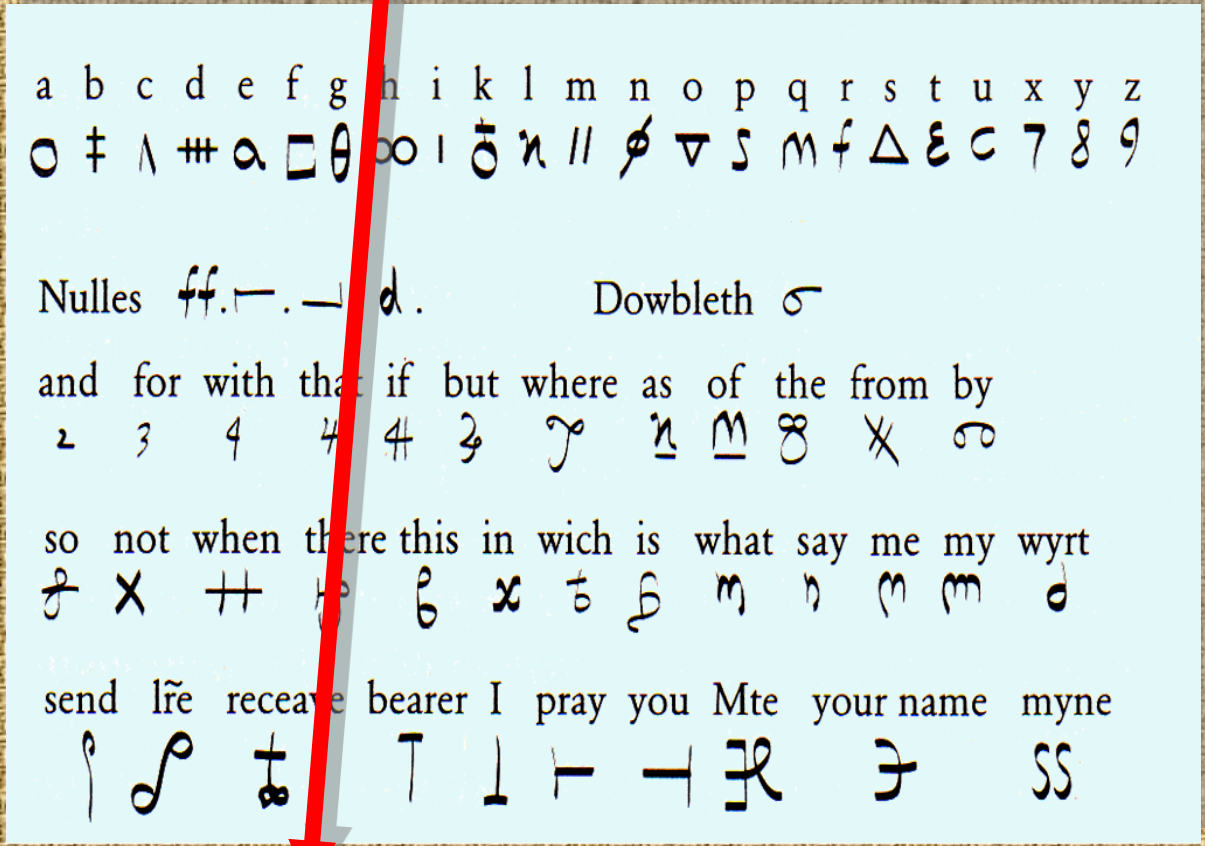
Le livre des Codes. Sélection du Reader’s Digest. Bagneux, 2009. p.66.

La cryptographie.

Le chiffrement par <u>substitution de lettres</u>.

Nomenclature: alphabet chiffré + mots chiffrés.

Marie Stuart, reine d'Écosse.



Anthony Babington.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.54-70.

Code: remplacer mot ou phrase par un autre mot, un symbole, un geste, un chiffre,…

Elisabeth Tudor, reine d'Angleterre.

Cryptanalyse: Thomas Phelippes.

Décapitation: 8 février 1587.

La cryptographie.

Le chiffrement par substitution de lettres.

Chiffre de César décalé de 3 lettres

Alphabet clair	Alphabet chiffré
A	D
B	E
C	F
D	G
E	H
F	I
G	J
H	K
I	L
J	M
K	N
L	O
M	P
N	Q
O	R
P	S
Q	T
R	U
S	V
T	W
U	X
V	Y
W	Z
X	A
Y	B
Z	C

Le chiffre de César: 3.

25 possibilités de chiffrement.

25 tentatives pour le déchiffrement !!!!

DES RENFORTS
ONT ÉTÉ ENVOYÉS

Texte clair

GHV UHQIRUWV
RKW HWH HQYRBHV

Texte chiffré par décalage de 3 lettres.

Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.103.

Les codes secrets décryptés. D.Müller. City Editions 2007.p.117-122.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Décalage vers la gauche de 3 lettres.

L'algorithme du chiffrement: la substitution de lettres par décalage.

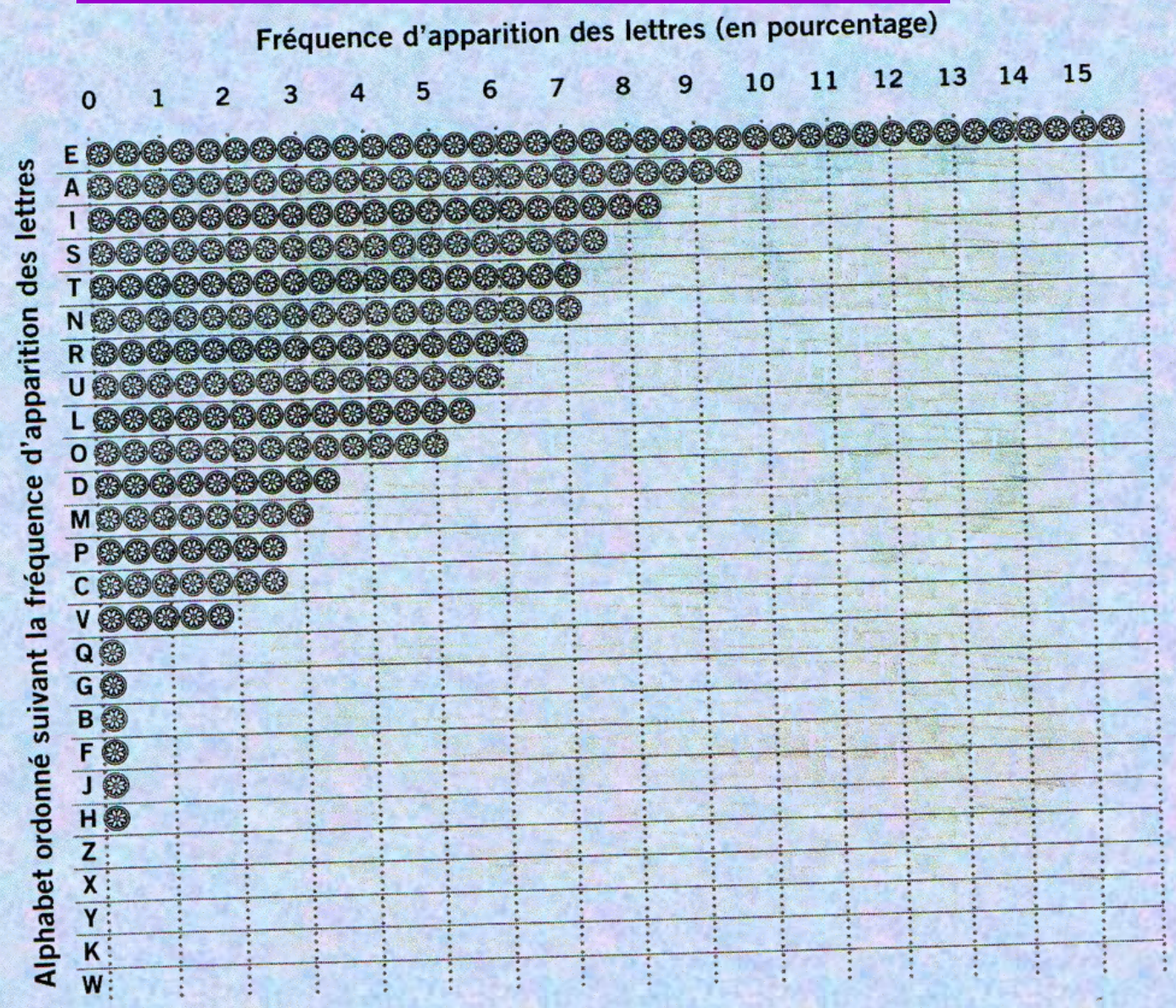
La clé du chiffrement: 3 à gauche.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.28

Le chiffre de César

Message clair	a	v	e	c	e	s	a	r
Message chiffré	D	Y	H	F	H	V	D	U
Numérisation: D=1	1	22	5	3	5	19	1	18

Analyse fréquentielle du français.



Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.68.

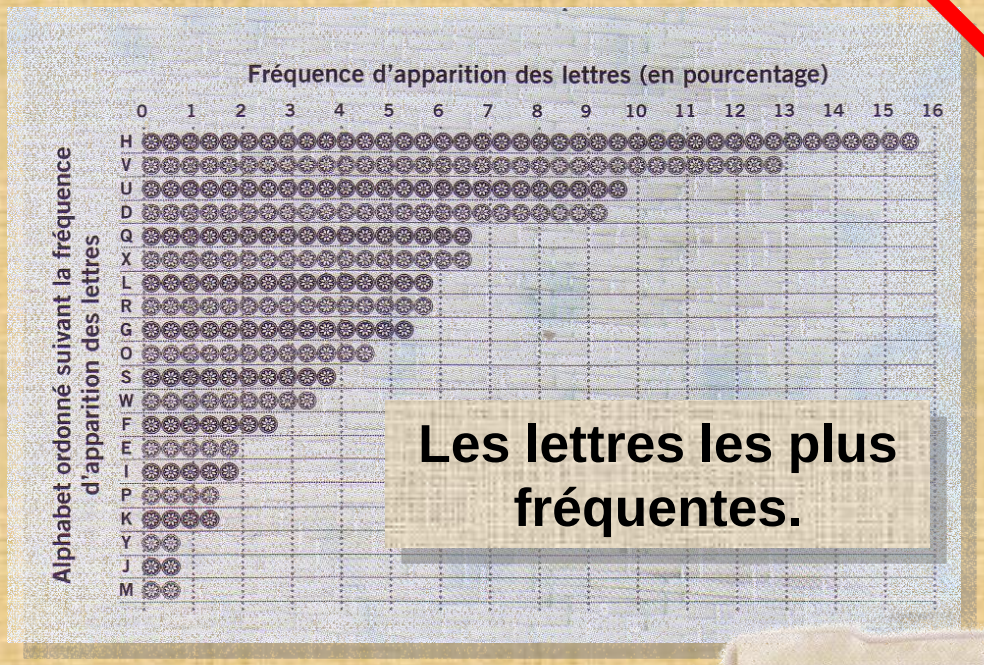
EAISTNRULODMPCV… **Et le cryptanalyste….**

Analyse fréquentielle du français.

Et le cryptanalyste….

Texte codé par chiffre de César de 3.

DSUHV DYRLU GHMHXQH GDQV XQH DXEHUJH, LOV DOOHUHQW IDLUH XQ WRXU DX PDUFKH. O'DERQGDQFH GH SURGXLWV IUDLV SURSRVHV VXU OHV HWDOV GHV SULPHXUV, GHV SRLVVRQQLHUV HW GHV ERXFKHUV OHV IDVFLQD.



Les lettres les plus fréquentes.

Les combinaisons de lettres fréquentes.

Après avoir déjeuné dans une auberge, ils allèrent faire un tour au marché. L'abondance de produits frais proposés sur les étals des primeurs, des poissonniers et des bouchers les fascina.

Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.69.

Chiffrement par substitution.

La substitution homophonique:

Texte clair	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					
Texte chiffré/ chiffre de César avec un décalage de 11 lettres	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K					
Homophones numériques des lettres fréquentes	6	1	4	5	2	3
	12	7	10	11	8	9
	18	13	16	17	14	15

La grille de chiffrement construite ici combine un chiffre de César de décalage 11 à trois homophones numériques des six lettres les plus fréquentes de la langue française (a, e, i, n, s, t).

Texte clair	ce	métier	est	difficile	à	exercer
Texte chiffré	NP	X1ET7C	13D3	O4QQ10N16WP	L	1I7CN13C

Dans le texte clair, la lettre *e* apparaît 8 fois. Lorsque l'on chiffre ce texte, il faut donc utiliser le cycle d'homophones attribué à la lettre *e*: P, 1, 7, 13, P, 1, 7 et 13.

Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.71.

Le disque de Léon Alberti (15ème s.)… et Confédérés Américains (fin 18ème s.).

Première machine cryptographique.

Alphabet clair: disque interne fixe.

Alphabet chiffré: disque externe mobile, vers droite ou gauche.

Mono alphabétique.

chiffrement: chiffre de César = 17
R (ext) = A (int).

clair	g	o	n	d	o	l	e
chiffré	X	F	E	U	F	C	V

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. p.47.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.72, 162-165.

Léon Alberti (1404-1472)

Le chiffrement par **substitution de lettres.**

Crypter: GONDOLE

Poly alphabétique.

Alternance.

Deux ou plusieurs alphabets chiffrés superposés.

1er alphabet: chiffre César: 5

2ème alphabet: chiffre César: 6

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
F	Z	B	V	K	I	X	A	Y	M	E	P	L	S	D	H	J	O	R	G	N	Q	C	U	T	W
G	O	X	B	F	W	T	M	Q	I	L	A	P	Z	J	D	E	S	V	Y	C	R	K	U	H	N

g	o	n	d	o	l	e
X	J	S	B	D	A	K

Histoire des codes secrets.
S.Singh. Éditions Jean-Claude Lattès, 1999, Paris. p.72, 162-165.

Léon Alberti (1460)

Poly alphabétique.

Mot-clef: LÉON.

Chiffrer: gondole.

(int) a-----→L (ext): lettre G (int) cryptée = (ext): R

(int) a-----→E (ext): lettre O (int) cryptée = (ext): S

(int) a-----→O (ext): lettre N (int) cryptée = (ext): B

(int) a-----→N (ext): lettre D (int) cryptée = (ext): Q

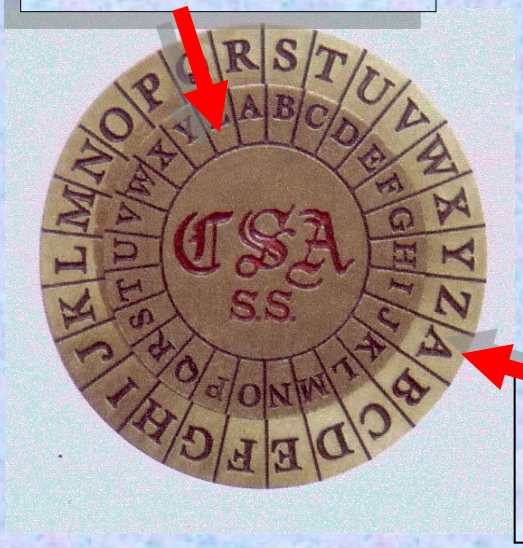
(int) a-----→L (ext): lettre O (int) cryptée = (ext): Z

(int) a-----→E (ext): lettre L (int) cryptée = (ext): P

(int) a-----→O (ext): lettre E (int) cryptée = (ext): S

g	o	n	d	o	l	e
L	E	O	N	L	E	O
R	S	B	Q	Z	P	S

Alphabet clair: disque interne fixe.



Alphabet chiffré: disque externe mobile, vers droite ou gauche.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. p.47.

Polyalphabétisme.

Abbé Johannes Heidenbert dit Jean Trithème (1528).

Blaise de Vigenère (1523-1596), diplomate français.

1ère ligne : lettre du texte clair: *gondole.*

1ère colonne: même lettre du mot à chiffrer: *gondole.*

Intersection: lettre chiffrée.

g	***o***	***n***	***d***	***o***	***l***	***e***
M	C	A	G	C	W	I

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.75-78; 95-110.

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.157.

Carré de Vigenère

Clair	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
1	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	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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
26	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

Version moderne du carré de Vigenère.

Carré de Vigenère avec clef. (1523-1596).

Mot-clef: LEON

1ère ligne: lettre du texte clair.

1ère colonne: lettre de la <u>clef</u> qui donne la ligne à utiliser.

Intersection: lettre chiffrée.

Le g (1ère ligne) x ligne L (1ère colonne) = R

clef	L	E	O	N	L	E	O
clair	***g***	***o***	***n***	***d***	***o***	***l***	***e***
crypté	R	S	B	Q	Z	P	S

Carré de Vigenère

Clair	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
1	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 A
2	C D E F G H I	J K L M N O P Q	R S T U V W X Y Z A B
3	D E F G H I J	K L M N O P Q R	S T U V W X Y Z A B C
4	E F G H I J K	L M N O P Q R S	T U V W X Y Z A B C D
5	F G H I J K L	M N O P Q R S T	U V W X Y Z A B C D E
6	G H I J K L M	N O P Q R S T U	V W X Y Z A B C D E F
7	H I J K L M N	O P Q R S T U V	W X Y Z A B C D E F G
8	I J K L M N O	P Q R S T U V W	X Y Z A B C D E F G H
9	J K L M N O P	Q R S T U V W X	Y Z A B C D E F G H I
10	K L M N O P Q	R S T U V W X Y	Z A B C D E F G H I J
11	L M N O P Q R	S T U V W X Y Z	A B C D E F G H I J K
12	M N O P Q R S	T U V W X Y Z A	B C D E F G H I J K L
13	N O P Q R S T	U V W X Y Z A B	C D E F G H I J K L M
14	O P Q R S T U	V W X Y Z A B C	D E F G H I J K L M N
15	P Q R S T U V	W X Y Z A B C D	E F G H I J K L M N O
16	Q R S T U V W	X Y Z A B C D E	F G H I J K L M N O P
17	R S T U V W X	Y Z A B C D E F	G H I J K L M N O P Q
18	S T U V W X Y	Z A B C D E F G	H I J K L M N O P Q R
19	T U V W X Y Z	A B C D E F G H	I J K L M N O P Q R S
20	U V W X Y Z A	B C D E F G H I	J K L M N O P Q R S T
21	V W X Y Z A B	C D E F G H I J	K L M N O P Q R S T U
22	W X Y Z A B C	D E F G H I J K	L M N O P Q R S T U V
23	X Y Z A B C D	E F G H I J K L	M N O P Q R S T U V W
24	Y Z A B C D E	F G H I J K L M	N O P Q R S T U V W X
25	Z 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
26	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

2 → 4 → 3 → 1 →

Version moderne du carré de Vigenère.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.75-78; 95-110.

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.157.

Le carré de Polybe.

En utilisant le carré de Polybe (IIème siècle av JC) le mot ‘’code’’ devient:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

‘’code’’

‘’13 34 14 15’’

Le livre des Codes. Sélection du Reader’s Digest. Bagneux, 2009. p.78.

Carré de Polybe - Wikipédia

Guerre 14-18

1 juin1918

Le code allemand ADFGVX.
Offensive du 1 juin 1918 -Cne Georges-Jean Painvin.

Radiotélégramme Morse

2 juin 1918: déchiffrement du code.

8 = AA p = AD

a	t	t	a	q	u	e	1	0	h
DV	DD	DD	DV	XX	GD	XD	AV	XG	DX

Clef de substitution

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Clef de transposition

M	A	I	S
DV	DD	DD	DV
XX	GD	XD	AV
DX	XX	XX	XX

Colonnes: ordre alphabétique

A	I	M	S
DD	DD	DV	DV
GD	XD	XX	AV
XX	XX	DX	XX

En morse, les lettres ADFGVX sont très distinctes.

Message final:

DD GD XX DD XD XX DV XX DX DV AV XX

Radiogramme de la Victoire - Annales des Mines

Le génie de Georges Jean Painvin - Familles

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.138-141, 466-467.

Les codes secrets décryptés. D.Müller. City Editions 2007.p.276-289.

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.181-189.

Guerre 14-18

Code ÜBCHI

3 août 1914 – déc.1914: code ÜBCHI
(Armée de Terre): mot-clef = chiffre-clef.

(D.Müller.p.281.p.77).

(H.Lehning. p.131-135.p.177-181).

Code ABC

21 janv 1915: mémoire de Cne George-Jean Painvin (1886-1980).

Code Vigenère de clef ABC.
(D.Mûller: p.284) (H.Lehning: p.179-180) .

Code ABCD

Code Vigenère de clef ABCD.
(D.Mûller: p.284). (H.Lehning. p.180).

50% faux messages.

Code KRU

1917- 5 mars 1918. (D.Mûller: p.284-285).

Code Fleissner

Grille tournante. D.Mûller: p77

Code ADFGX.

5 mars 1918

Colonel Fritz Nebel: code GEDEFU 18:
GEheimeschrift DEr FUnker 18:
carré de Polybe: I et J confondus, V et W séparés.
(H.Lehning: p.181-185) (D.Mûller: p.276-289).

5 avril 1918: décryptement par le Cne G-J Painvin (1886-1980).

Code ADFGVX.

1 juin 1918

(H.Lehning . p.186-189).

26 lettres+10 chiffres.

Les codes secrets décryptés. D.Müller. City Editions 2007.

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.179131-135.p.181-185.

Les machines à coder et décoder

Cylindre de Jefferson (1743-1826).

Cylindre de Cdt Étienne Bazeries (1846-1931). Décryptage Gaëtan Viaris.

H.Lehning.p.195-197.

La machine à chiffrer M-94 de l'U.S. Army sur le champ de bataille.1922-1943.

25 disques.

Mot-clef quotidien de 25 lettres.

***Jefferson* Wheel Cypher & US *M-94* Cipher - Cipher Machines**

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.191-197.

Les codes secrets décryptés. D.Müller. City Editions 2007.p.256-257.

2ème guerre mondiale

USA Army: 1940 – 1953 (Corée).

CSP-1500 US Navy.

Hagelin M-209 US Army

Portable.

Morse.

Magic (cryptography) - Wikipedia, the free

Machines a chiffrer version Hagelin - header

The ***B-211*** cipher ***machine*** - Passagen

Hagelin B-21 - Crypto Museum

Boris Hagelin

***M-209* - Wikipedia, the free encyclopedia**

2ème guerre mondiale

France 1930 - 1962: matériel suédois: Boris Hagelin: machine C-36; C-37(Marine); machine B-211; machine M-209 (Algérie).

Machine Hagelin C-36.

•***World War*** II cryptography - Wikipedia, the free encyclopedia

C-36 (cipher ***machine***) - Wikipedia, the free encyclopedia

C-36 - Wikipédia

French Hagelin cipher ***machines*** - Christos military and

Boris Hagelin - Wikipédia

2ème guerre mondiale **3ème Reich** **Japon** **Enigma**

Général Guderian. Campagne de France, 1940. Enigma à 3 rotors.

Soldats allemands transcrivant un message sur Enigma.

Module à quatre rotors.

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.198.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. p.63.

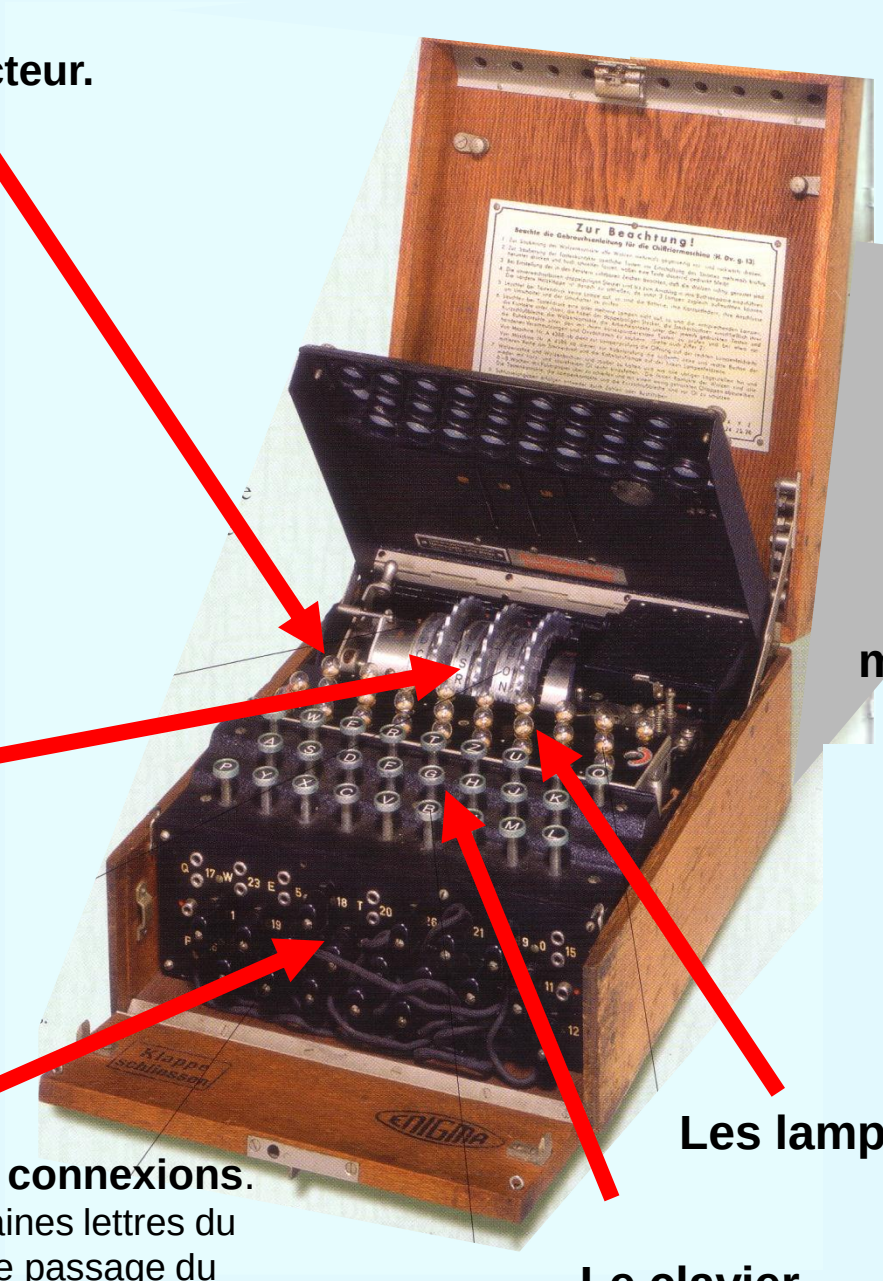
ENIGMA

1926

Le réflecteur.

Les rotors brouilleurs.
26 lettres.
Position de départ selon le chiffre du jour.

Le pupitre de connexions.
Il permute certaines lettres du clavier avant le passage du texte dans les rotors.



Les lampes.

Le clavier.

Enigma fut breveté en 1918 par Arthur Sherbius pour un usage commercial et complexifié par l'Etat-Major allemand.

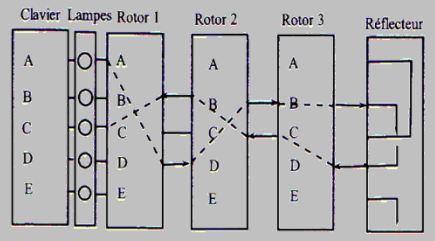
Le paramétrage: tous les matins, en fonction du chiffre du jour, changement des rotors brouilleurs

Premier message avec les paramètres du chiffre du jour pour donner les nouveaux paramètres des rotors brouilleurs.

Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.116.

Chaque récepteur-émetteur a le livre des clefs quotidiennes.

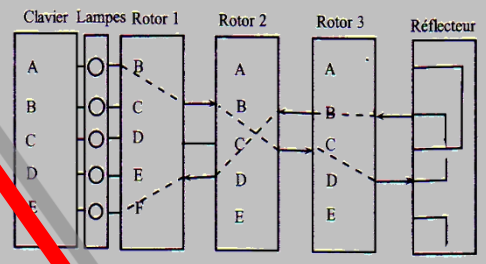
Chiffrage du message



position AAA. L'appui sur la touche A allume la lampe « C ».

Clef du jour: HXA.

Opérateur chiffre AWO, qu'il a choisi, avec la clef HXA.



ENIGMA en position BAA.

Le message commence par six lettres correspondant à AWO chiffrée avec la clef du jour (HXA), suivies du texte chiffré avec la clef AWO. [AWOAWO]

Taper le texte: à chaque lettre frappée, noter la lettre qui s'allume.

L'opérateur émet le message avec sa clef AWO.

Envoyer le cryptogramme obtenu.

Initiation à la cryptographie. G. Dubertret. Édition Vuibert, Paris, 2012.p.59-62

Déchiffrement

Positionner les rotors AWO.

Taper le cryptogramme reçu et noter les lampes qui s'allument.

Lire le message.

***Enigma* (machine) - Wikipédia**

Le ‘’cassage’’ d’ Enigma: ULTRA.

- 1926: Le bureau de cryptanalyse polonais, Biuro Szyfrow: linguistique +mathématiques.
- 8 nov 1931: 2ème Bureau: plans de la machine. Clefs du jour à major Gwido Langer. Marian Rejewski et ses ‘’Bombes’’ finissent par déchiffrer les messages.
- Déc.1938 l’ajout de 2 rotors brouilleurs et l’extension du pupitre de connexions: case départ.
- 19 août 1939: deux répliques d’ Enigma et les analyses de Rejewski sont convoyées à Londres.
- 10 mai 1940 changement du protocole d’émission.
- 1940: Le centre de Bletchley Park (Comté de Buckingham G.B.): Quartier général de l’école gouvernementale des codes et chiffres (Bureau 40).

Les casseurs de codes (de la seconde guerre mondiale). Sinclair McKay. Éditions, Ixelles Publishing SA, 2012.p.96,…

- 1942: Alan Turing (1911- 1954) et les ‘’Bombes’’.

Les ‘’cillis’’: messages prévisibles et les mots probables (cribs)

exe: pose de mines exe: messages météo ‘’Wetter’’. Cilli, la petite amie.

L’erreur humaine: opérateurs qui utilisent les mêmes mots-clés de début de message.

Du boulier à la révolution numérique. V. Torra. Collection ‘’Le Monde est Mathématique’’ éditée par RBA France, SARL, Paris. 2013. Tome 13.p.110-115.

Les prises de machines et de clefs sur les sous-marins ou les navires météorologiques allemands.

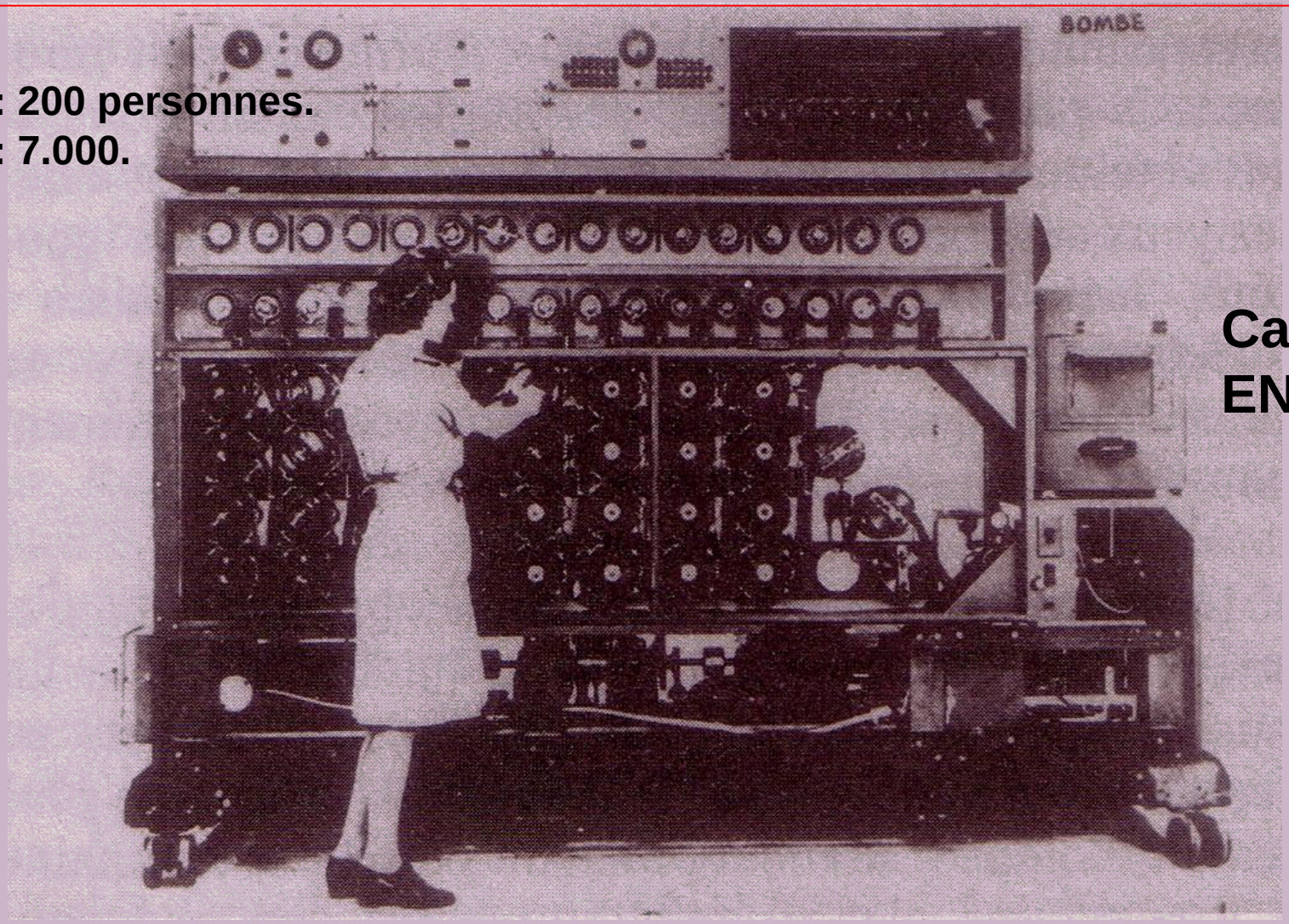
Le livre des Codes. Sélection du Reader’s Digest. Bagneux, 2009. p.121.

Codage et cryptographie. J.Gomez. Collection ‘’Le Monde est Mathématique’’ éditée par RBA France, SARL, Paris. 2013. T2. p.62-74.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris. p.165-241.

Centre de Bletchley Park (Comté de Buckingham G.B.)et ses ‘’*Huttes*”:

1940: 200 personnes.
1945: 7.000.



Casser ENIGMA.

Premier prototype de ‘’bombe” (Rejewski - Turing : 14 mars 1940).

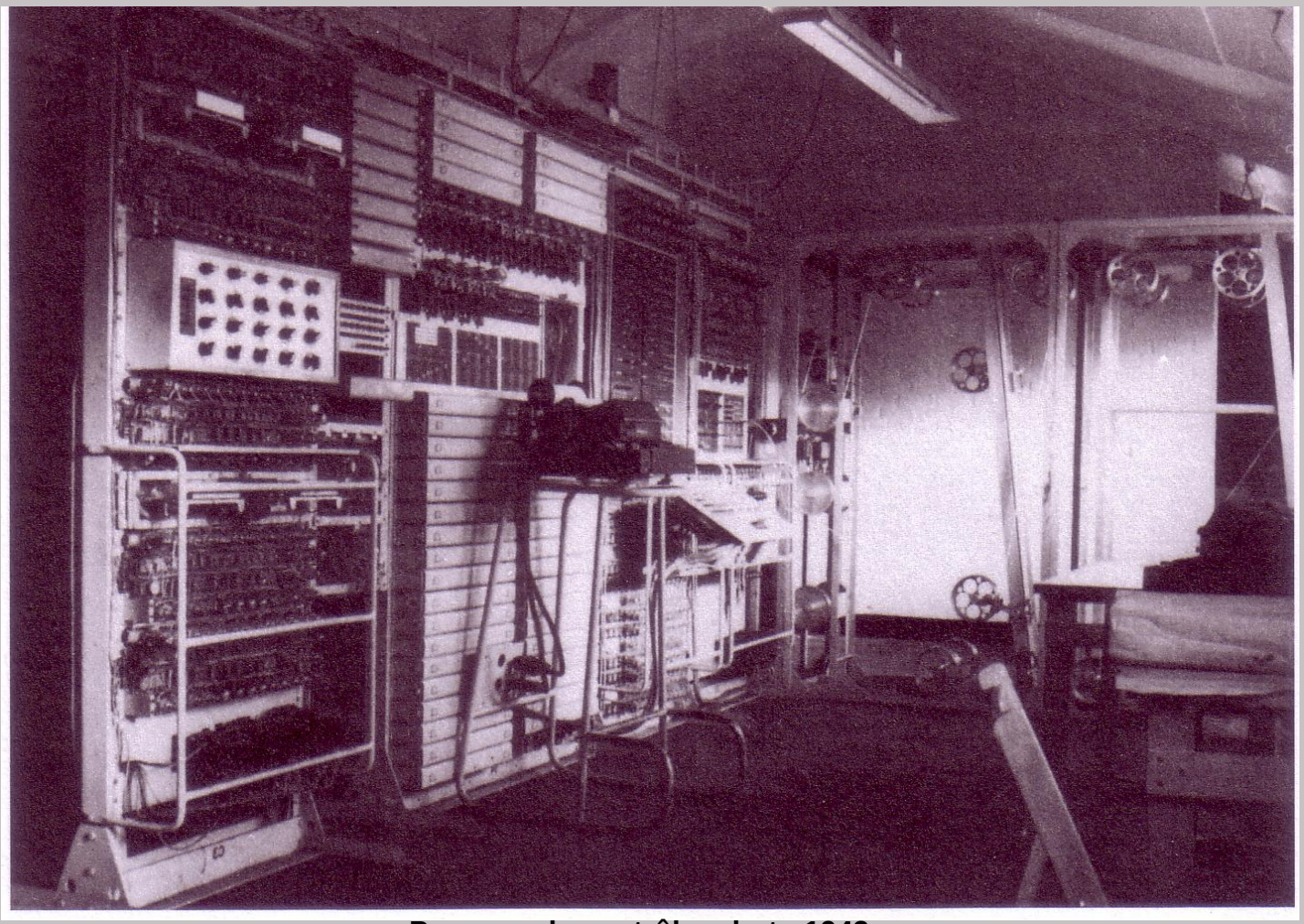
Fin 1942: 49 ‘’bombes”(Rejewski – Turing).

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris. p.226.

Centre de Bletchley Park (Comté de Buckingham G.B.) 8 déc 1943:

Colossus **Max Newman, Tommy Flovers.**

1.500 valves électroniques: tubes à vide.



Panneau de contrôle: photo 1943.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. T2.p73.

Casser la Machine de LORENTZ.

1974 !

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris. p.303-305.

Les *Navajo Code – Talkers*: les parleurs en code.

1ère guerre mondiale: 8 membres de la tribu Choctaw: 36ème Division US.

2ème guerre mondiale: essais: locuteurs basques, gallois, améridiens.

7 déc 1941: Pearl Harbour.

Mars 1942: Philip Johnston. LCL *Marines* James E. Jones.

29 Navajos

420 Navajos formés aux transmissions et intégrés dans les divisions de Marines US (1942-1945).
Guerre de Corée (1950-1953).
Code navajo secret jusqu'en 1968.
14 Comanches lors du débarquement en Normandie.

La langue navajo très imagée avec une grammaire complexe est propice à la création d'un vocabulaire cryptique facile à mémoriser.

Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.123.

Les *Navajo Code – Talkers.*

Les ‘’radiocodeurs” Navajos.

Le code navajo

Lexique: 274 + 234 = 508 mots

Chasseur	Oiseau-mouche	*Da-he-tih-hi*
Avion d'observation	Chouette	*Ne-as-jah*
Avion d'assaut	Hirondelle	*Tas-chizzie*
Bombardier	Buse	*Jay-sho*
Bombardier en piqué	Faucon	*Gini*
Bombes	Œufs	*A-ye-shi*
Véhicule amphibie	Grenouille	*Chal*
Cuirassé	Baleine	*Lo-tso*
Destroyer	Requin	*Ca-lo*
Sous-marin	Poisson en fer	*Besh-lo*

Tableau 11 Noms de code navajos pour les avions et les bateaux.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris. p.249.

Inconvénients: 1) lexique
2) Dzeh =e: fréquence: utilisation d’homophones de e, t, a, o, i, n.

Alphabet.

Code alphabétique Navajo

A	Ant (fourmi)	*Wol-la-chee*
B	Bear (ours)	*Shush*
C	Cat (chat)	*Moasi*
D	Deer (daim)	*Be*
E	Elk (élan)	*Dzeh*
F	Fox (renard)	*Ma-e*
G	Goat (chèvre)	*Klizzie*
H	Horse (cheval)	*Lin*
I	Ice (glace)	*Tkin*
J	Jackass (baudet)	*Tkele-cho-gi*
K	Kid (chevreau)	*Klizzie-yazzi*
L	Lamb (agneau)	*Dibeh-yazzi*
M	Mouse (souris)	*Na-astso-si*
N	Nut (noisette)	*Nesh-chee*
O	Owl (chouette)	*Ne-as-jah*
P	Pig (cochon)	*Bi-sodh*
Q	Quiver (carquois)	*Ca-yeilth*
R	Rabbit (lapin)	*Gah*
S	Sheep (mouton)	*Dibeh*
T	Turkey (dinde)	*Than-zie*
U	Ute (Peau-Rouge)	*No-ad-ih*
V	Victor (vainqueur)	*A-keh-di-glini*
W	Weasel (belette)	*Gloe-ih*
X	Cross (croix)	*Al-an-as-dzoh*
Y	Yucca (yucca)	*Tsah-as-zih*
Z	Zinc (zinc)	*Besah-do-gliz*

Le livre des Codes. Sélection du Reader’s Digest. Bagneux, 2009. p.123.

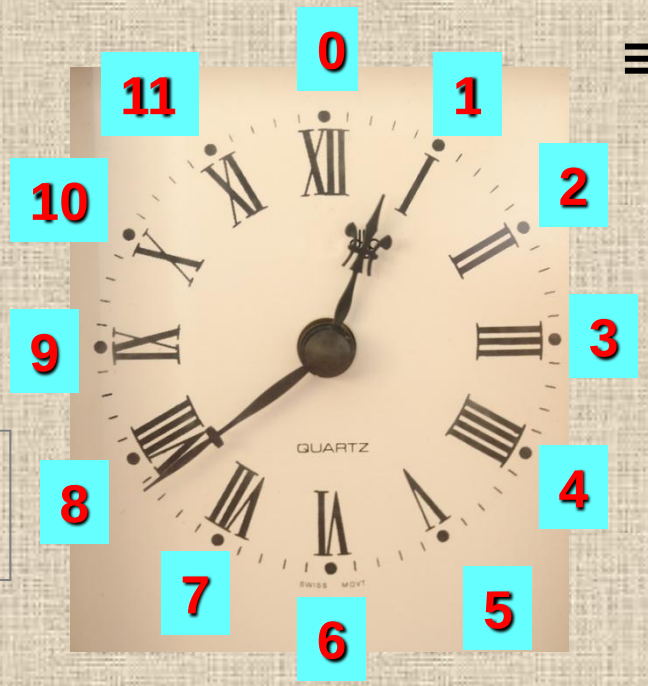
Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris. p.245-255.

Addition modulaire (modulo).

L'horloge:

Arithmétique modulaire

≡



3 (heures) + 2 (heures) ≡ 5 (modulo 12)

9 (heures) + 8 (heures) ≡ 5 (modulo12)
9+8=17 / 12= 1 reste 5.

11 (heures) + 10 (heures) ≡ 9 (modulo12)
11+10=21 / 12= 1 reste 9.

0 (heures) + 30 (heures) ≡ 6 (modulo 12)
30/12 = 2 reste 6.

Multiplication modulaire (modulo).

3 x 3 ≡ 2(modulo 7) 9/7 = 1 reste 2.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. Tàme 2. p.29-39.

x	1	2	3	4	5	6
3^x	3	9	27	81	243	729
3^x (mod 7)	3	2	6	4	5	1

la fonction est erratique en modulo.

$453^x \equiv 5\,787$ (modulo 21 997). Trouver x ?

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.324-329.

Le chiffre de César: 3

Codage et cryptographie. J.Gomez. Collection ‘’Le Monde est Mathématique’’ éditée par RBA France, SARL, Paris. 2013.p.33-35.

≡

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

$$C(x) \equiv (x + k) \text{ (modulo } n)$$

C(x): valeur chiffrée.

x est le ‘’numéro’’ de la lettre.

k est la clef: ici 3.

$$C(x) \equiv x + 3 \text{ (modulo 26)}$$

C(11) (lettre L) $\equiv$ 11 + 3 $\equiv$ 14 (mod 26) qui correspond à O

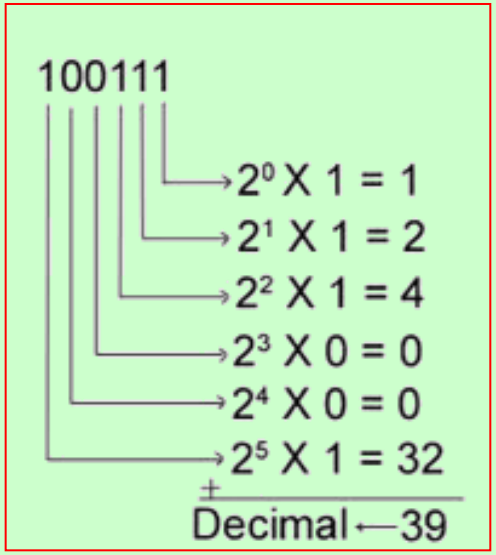
C(23) (lettre X): 23 + 3 = 26 $\equiv$ 0 (mod 26) [26/26=1 reste 0] : lettre A

C(25)(lettre Z) $\equiv$ 25 + 3 $\equiv$ 2 (modulo 26) [28/26=1 reste 2]
qui correspond à la lettre C.

Passage du système décimal (0123456789) au système binaire(0 et 1).

0 ou 1 = 1 bit (binary digit)

19	2	
1	9	2
1	4	2
0	2	2
0	1	



1 0 0 1 1

$1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0$

16 + 0 + 0 + 2 + 1 = 19

$19_{(10)} = 10011_{(2)}$

8 bits = 1 Octet = 00010011 = 19.

$33_{(10)} = 1x2^5+0x2^4+0x2^3+0x2^2+0x2^1+1x2^0 = 100001_{(2)}$ = ASCII = 00100001.

Afin de vous aider à protéger votre confidentialité, PowerPoint a empêché le téléchargement automatique de cette image externe. Pour la télécharger et l'afficher, cliquez sur Options dans la barre de message, puis cliquez sur Autoriser le contenu externe.

ASCII

Système hexadécimal et ASCII,…

0123456789ABCDEF

Les chiffres.

Binaire	Hexadécimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

77 s'écrit donc en base 2: 100 1101.

$$77_{(10)} = 1 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

$$77_{(10)} = 64 + 0 + 0 + 8 + 4 + 0 + 1$$

$$77_{(10)} = 1001101_{(2)}$$

Conversion de 77 en base 16:

77	16
13	4

$$= 4 \times 16^1 + 13 \times 16^0 = 4\ D$$

$$= 64 + 13 = 77$$

$$77_{(10)} = 004\ D_{(16)} = 0100\ 1101_{(2)}$$

- $16^0 = 1$
- $16^1 = 16$
- $16^2 = 256$
- $16^3 = 4096$
- $16^4 = 65536$

Les lettres.

Portail de l'informatique

American Standard Code for Information Interchange - Wikipédia

Les bases décimale, binaire et *hexadécimale* - Apprendre en ligne.net

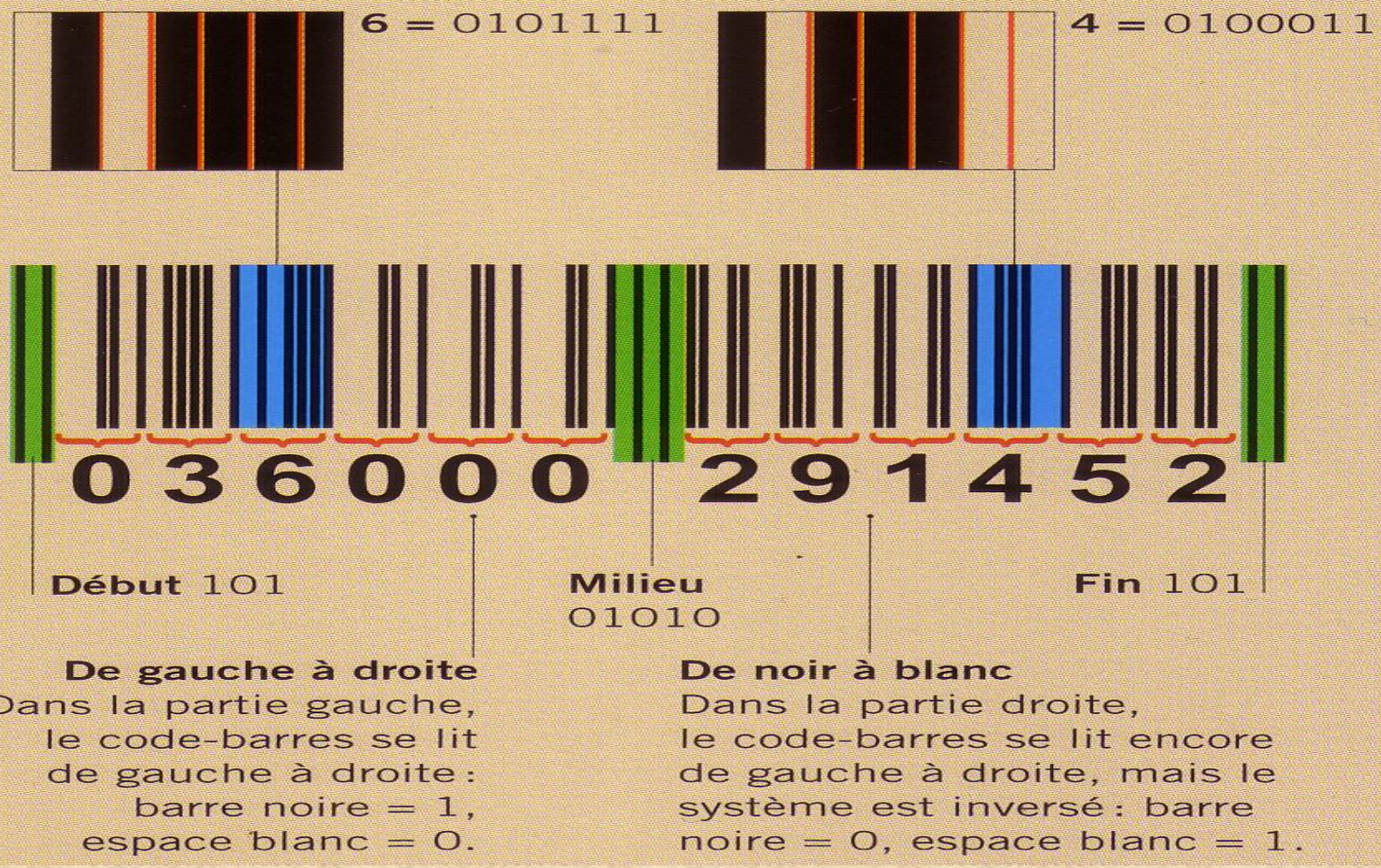
Système hexadécimal : définition et explications - Techno-Science.net

Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.205.

Le système du code-barres

0 0001101	**3** 0111101	**6** 0101111	**9** 0001011
1 0011001	**4** 0100011	**7** 0111011	
2 0010011	**5** 0110001	**8** 0110111	

Comment fonctionne le code-barres



ASCII

ASCII **(1970:Amecican Standard Code for Information Interchange): ''Ass-Key'' ''clef d'âne''.**

256 = 2^8 possibilités de 8 (octet): 0/1

Message crypté: transposition (bits permutés, remplacés dans les lettres); substitution; avec une clef.

TABLEAU ASCII

Caractère	Binaire	Déc.	Caractère	Binaire	Déc.	Caractère	Binaire	Déc.
	00100000	32	@	01000000	64	`	01100000	96
!	00100001	33	A	01000001	65	a	01100001	97
"	00100010	34	B	01000010	66	b	01100010	98
#	00100011	35	C	01000011	67	c	01100011	99
$	00100100	36	D	01000100	68	d	01100100	100
%	00100101	37	E	01000101	69	e	01100101	101
&	00100110	38	F	01000110	70	f	01100110	102
'	00100111	39	G	01000111	71	g	01100111	103
(	00101000	40	H	01001000	72	h	01101000	104
)	00101001	41	I	01001001	73	i	01101001	105
*	00101010	42	J	01001010	74	j	01101010	106
+	00101011	43	K	01001011	75	k	01101011	107
,	00101100	44	L	01001100	76	l	01101100	108
-	00101101	45	M	01001101	77	m	01101101	109
.	00101110	46	N	01001110	78	n	01101110	110
/	00101111	47	O	01001111	79	o	01101111	111
0	00110000	48	P	01010000	80	p	01110000	112
1	00110001	49	Q	01010001	81	q	01110001	113
2	00110010	50	R	01010010	82	r	01110010	114
3	00110011	51	S	01010011	83	s	01110011	115
4	00110100	52	T	01010100	84	t	01110100	116
5	00110101	53	U	01010101	85	u	01110101	117
6	00110110	54	V	01010110	86	v	01110110	118
7	00110111	55	W	01010111	87	w	01110111	119
8	00111000	56	X	01011000	88	x	01111000	120
9	00111001	57	Y	01011001	89	y	01111001	121
:	00111010	58	Z	01011010	90	z	01111010	122
;	00111011	59	[	01011011	91	{	01111011	123
<	00111100	60	\	01011100	92	|	01111100	124
=	00111101	61	]	01011101	93	}	01111101	125
>	00111110	62	^	01011110	94	~	01111110	126
?	00111111	63	_	01011111	95			

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.306-309.

ASCII

Exemple de message chiffré avec clef.

Message clair	h	e	l	l	o
Message en ASCII	01101000	01100101	01101100	01101100	01101111
Clef: david	01100100	01100001	01110110	01101001	01100100
Message chiffré	00001100	00000100	00011010	00000101	00001011
Message lu: HELLO	01101000	01100101	01101100	01101100	01101111

<u>Addition des chiffres binaires</u>: semblables = 0; différents = 1

0+0 ou 1+1 = 0

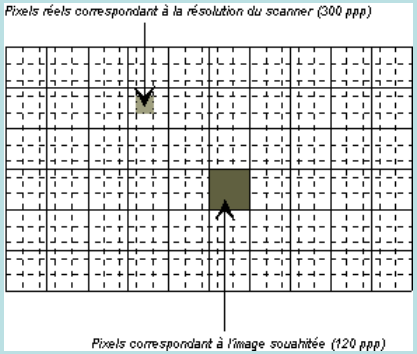
0+1 ou 1+0 = 1

Problèmes de l'algorithme et de la clef.

Histoire des codes secrets.
S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.308-309..

La numérisation des images.

Pixel: picture element.



1.1. ***Numérisation*** **d'une grandeur physique fixe - CNDP**

Les images noir et blanc.

256 niveaux de gris sur une profondeur de 8 bits par pixel.

Les couleurs.

256 niveaux de couleur. Le pixel codé sur 24 bits:
en RVB(rouge, vert, bleu) en photographie;
en CMJN(cyan, magenta, jaune, noir) en infographie.

	R	V	B		C	M	J	N
Azur	0	127	255		100	50	0	0
Beige	245	245	220		0	0	10	4
Cyan	0	255	255		100	0	0	0
Lavande	230	230	250		8	8	0	2
Saumon	255	140	105		0	45	59	0

Couleurs en RVB et CMJN.

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.227.

Le son.

Analyse de la période: Hertz par seconde.

44 100 bits par seconde: qualité CD

Radio: 22 000 Hertz / s. **Téléphone: 8 000 H/s.**

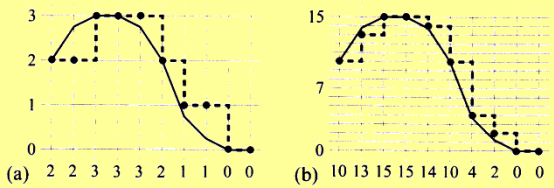


Figure 17.14 En (a), un signal est échantillonné sur 4 bits, les erreurs sont importantes. En (b) un plus grand nombre de bits diminue fortement les erreurs.

Le radio-amateur. Olivier Pilloud. Éditions Technip, Paris, 2007. 3ème édition.p.275.

Film – Vidéo…

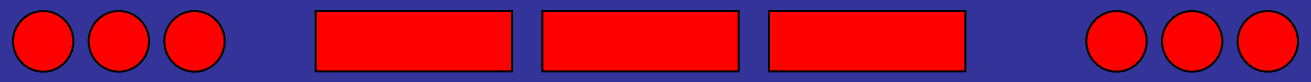
Succession d'images fixes, à une fréquence de 25 ou 30 images fixes par seconde.

Disque compact - Wikipédia

Le code Morse Samuel (1791-1872)

Impulsions électriques: brèves, longues, espaces entre lettres et mots.

Transmission filaire , télégraphique



''SAVE OUR SOULS''

''SAVE OUR SHIP''

1ère utilisation en guerre: guerre de Crimée (1853-1856) par journaliste du Time.

5ème Symphonie de Beethoven: Victory.

Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.96-97.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013.p.55-59.

A D
P
F
G
V
X

A	·—	J	·———	S	···	2	··———
B	—···	K	—·—	T	—	3	···——
C	—·—·	L	·—··	U	··—	4	····—
D	—··	M	——	V	···—	5	·····
E	·	N	—·	W	·——	6	—····
F	··—·	O	———	X	—··—	7	——···
G	——·	P	·——·	Y	—·——	8	———··
H	····	Q	——·—	Z	——··	9	————·
I	··	R	·—·	1	·————	0	—————

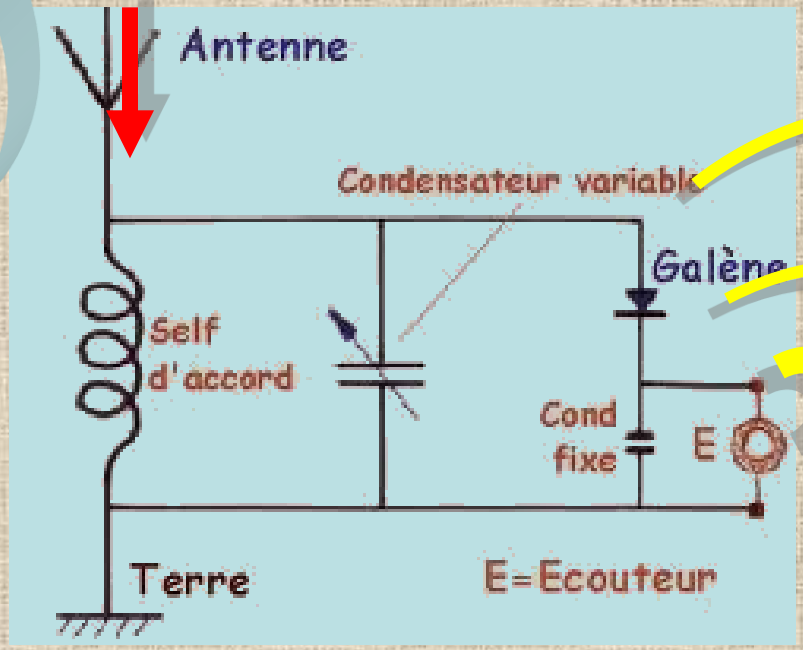
Le grand livre des codes secrets. M. Piquemal, D. Royo. Illustrations C. Dutertre. Albin Michel Jeunesse, Paris, 2004.

Poste à galène.

Réception d'ondes radio

Galène: sulfure de Pb.

Signal électronique.



Ondes sonores.

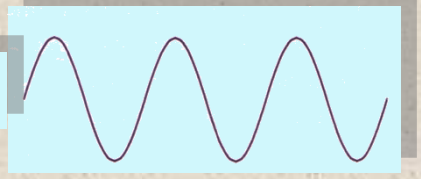
Ondes électromagnétiques.

Selon antenne: GO, PO.

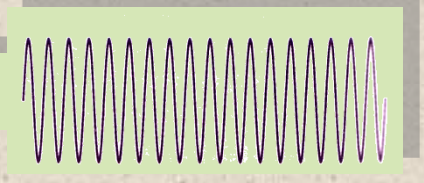
Récepteur à cristal - Wikipédia

Ondes Photoniques.

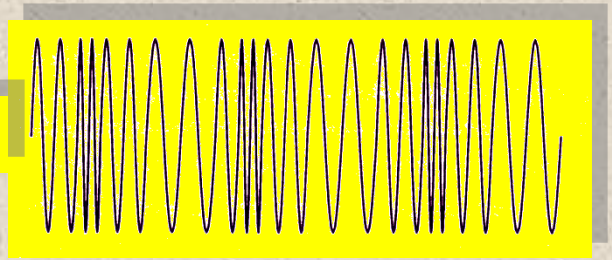
Basse Fréquence.

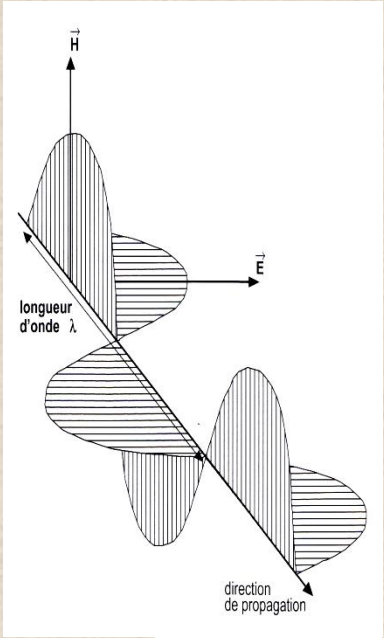


Haute Fréquence.



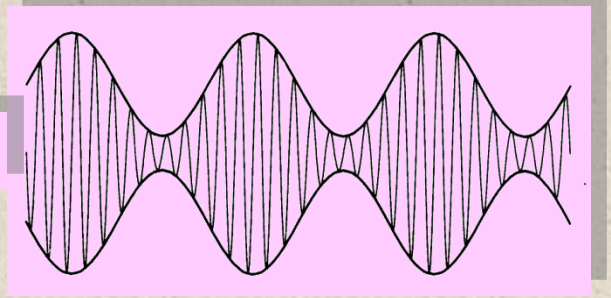
Modulation de fréquence.





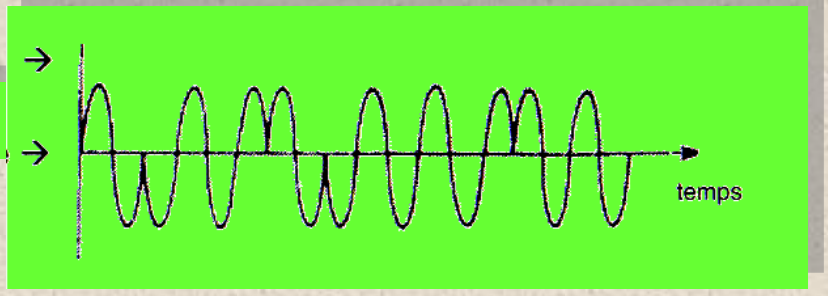
Champs électromagnétiques , environnement et santé. Sous la direction de A.Perrin, M.Souques. Édtions Springer-Verlag, Paris, 2011.p.6

Modulation d'amplitude.



Au cœur des ondes. Les champs électromagnétiques en question. F. Ndagijimana, F.Gaudaire. Éditions Dunod, Paris, 2013.p.40.

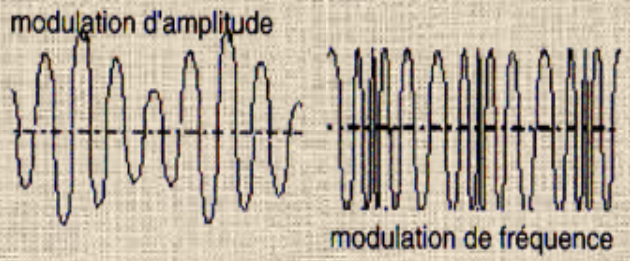
Modulation de phase.



Le radio-amateur. Olivier Pilloud. Éditions Technip, Paris, 2007. 3ème édition.p.282-283.

Modulations pour transmettre un signal analogique.

L'amplitude de l'onde varie en fonction du niveau du signal transmis.

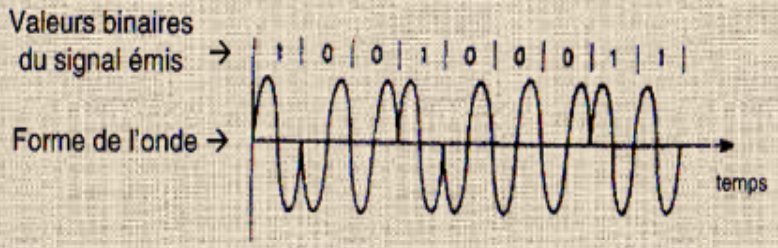


La fréquence de l'onde varie en fonction du niveau du signal transmis.

Modulations pour transmettre un signal numérique.

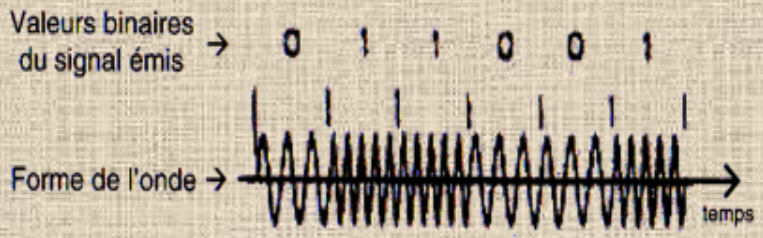
Modulation d'un signal numérique par déplacement de phase (PSK - *Phase Shift Keying*) :

L'information numérique est codée en changements de phases de l'onde radio

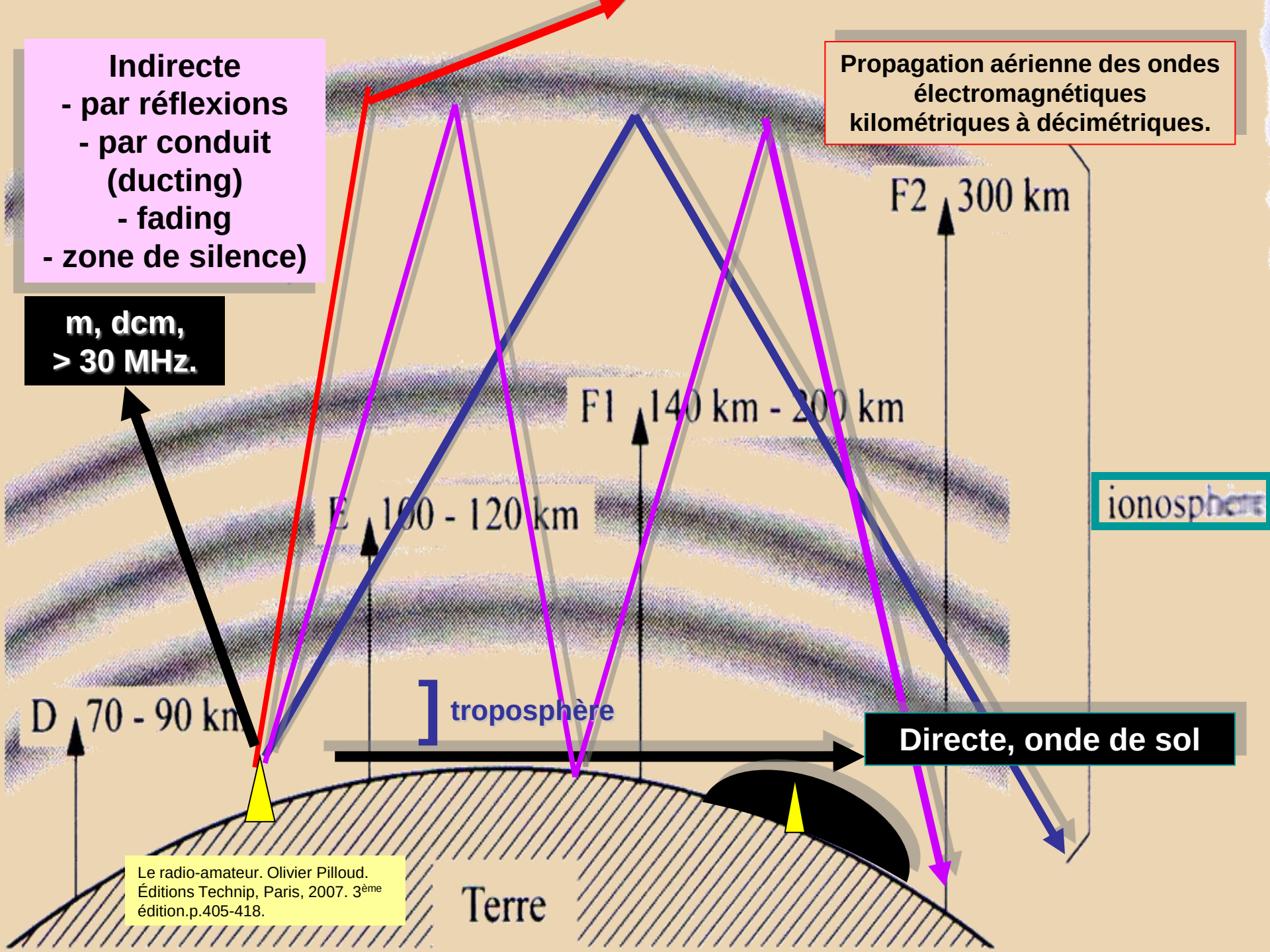


Modulation d'un signal numérique par déplacement de fréquence (FSK - *Frequency Shift Keying*) :

L'information numérique est codée en changements de fréquences de l'onde radio



Au cœur des ondes. Les champs électromagnétiques en question. F. Ndagijimana, F.Gaudaire. Éditions Dunod, Paris, 2013.p.40.



Le radio-amateur. Olivier Pilloud. Éditions Technip, Paris, 2007. 3ème édition.p.405-418.

‘’Les militaires français scrutent les colères du Soleil”.

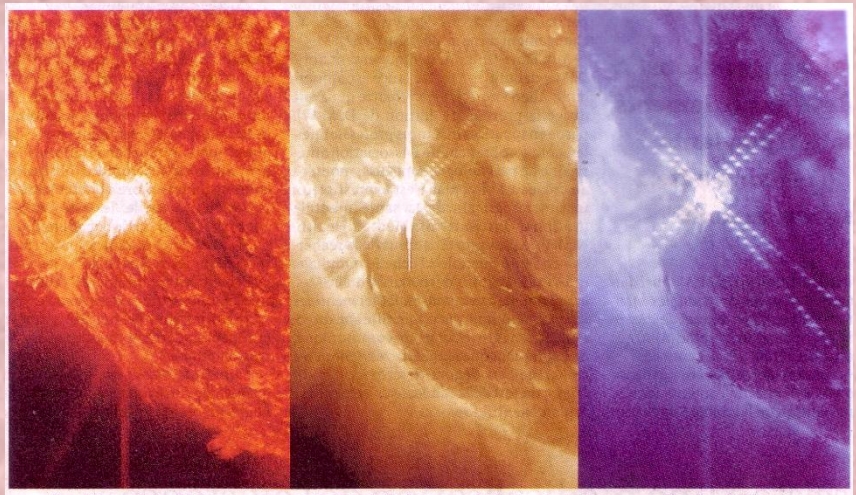
Commandement de la Défense Aériennes et des Opérations de l’Armée de l’Air (CDAOA).

SSN: Smoothed Sunspot Number.

Mars 2010: Adj-Chef Lionel Biree. Projet FEDOME
(Fédération des données de météorologie de l’espace) : système d’alerte « des perturbations des moyens de communication, de détection et de navigation par satellites » dues à l’activité solaire.

<u>11 nov 2012</u>: 02 h 16mn: ‘’ un filament de plasma…de la couronne solaire atteint le lendemain à 23 h 16 le satellite américain ACE, cinquante minutes plus tard la magnétosphère terrestre… …chute de six kilomètres de plusieurs satellites en orbite basse…‘’

<u>Conséquences</u>: …rupture des liaisons radio de haute fréquence…signaler…



Eruption solaire du 12 novembre 2012 : le Soleil photographié selon trois longueurs d’ondes différentes par le Solar Dynamics Observatory (SDO) de la NASA.

NASA/SDO/GODDARD SPACE

…avertir pour changer de fréquence…

Pilotes d’E3-F, avions Awacs français.

1991: opération DAGUET: un ordre d’engagement jamais parvenu !!!

Vahé Ter Minassian. Le Monde. Science & Médecine. 15 mai 2013.

Les transmissions.

Ondes acoustiques

Ondes électromagnétiques visibles.

etc…

Son, image, écriture.

Émission.

Signal électrique.

Signal électronique.

Les milieux: terre, mer, air, espace.

Morse.

Analogique

Numérique

Interception.

Lecture.

Filaire: cuivre, verre,…

Ondes électromagnétiques:

Téléphonie

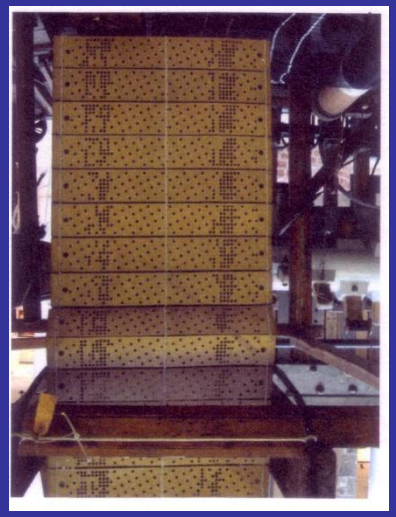
Télégraphie

Télévision

Réception

Son, image, écriture.

Chiffrement à flot.



MJ Jacquard (1752-1834).

Du boulier à la révolution numérique. V. Torra. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. Tome 13.p.96.

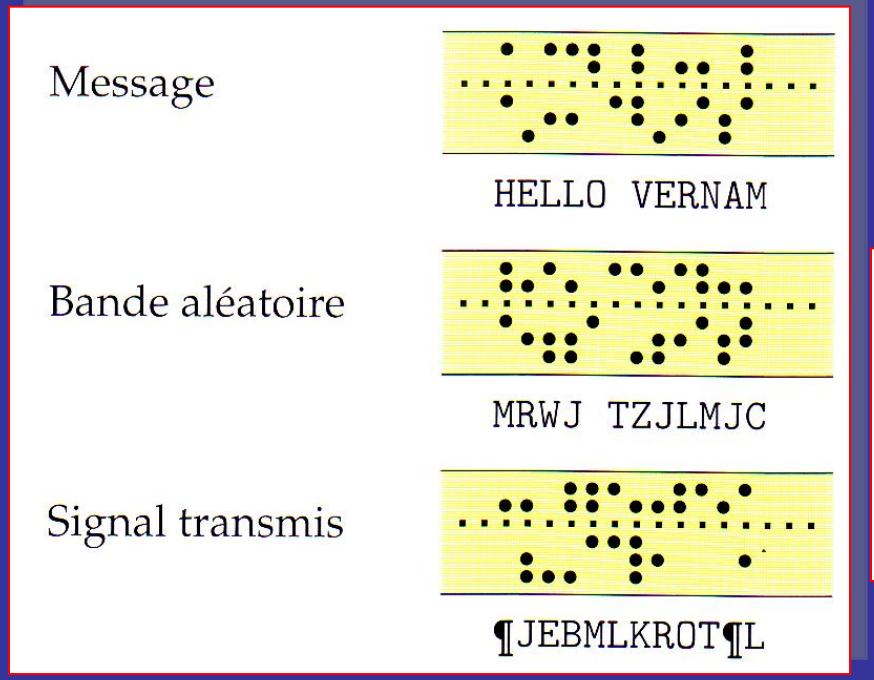
Système Vernam(1917).

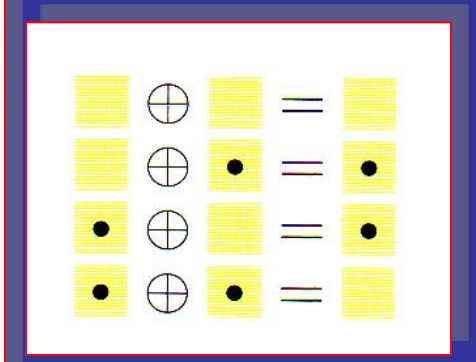
Téléscripteur: filaire, radio.

Symboles du message combinés à symboles d'une séquence pseudo-aléatoire identique chez l'émetteur et le récepteur.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. Tome 2.p.56.

Téléscripteur - Wikipédia





Bande aléatoire de même longueur que le message et utilisée une fois.

La cryptologie. P.Guillot. EDP Sciences 2013. p.26-28.

Cryptographie symétrique.

Chiffrement et déchiffrement : clef identique.

IBM *LUCIFER* (1970)

Accord préalable de l'émetteur et du receveur sur le chiffrement.

Chiffrement.

- **Message traduit en blocs de 64 bits.**
- **Brassage des bits de chaque bloc.**
- **Chaque bloc séparé en demi-blocs de bits.**
- **Permutation et substitution des bits : n cycles.**

Les codes secrets décryptés. D.Müller. City Editions 2007.p.317.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.310-315..

Déchiffrement. **Processus inverse du chiffrement.**

Solution (Feistel): D.E.S. (1976) : version 56 bits de LUCIFER (Data Encryption Standard). G. Dubertret.p.91-96.

Chacun a sa clef: multiplication des clefs et risques lors échanges.

IDEA (1992)(Internationational Data Encryption Algorithm) G. Dubertret.p.96-100.

AES (2000)(Advanced Encryption Standard) G. Dubertret.p.111-130.

Secret de l'échange du message et des clefs ?

Initiation à la cryptographie. G. Dubertret. Édition Vuibert, Paris, 2012.p.155.

Clefs de chiffrement et déchiffrement identiques ?

La cryptologie. P.Guillot. EDP Sciences 2013.p.36-37;p.45.

Authentification du message ?

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.310-315..

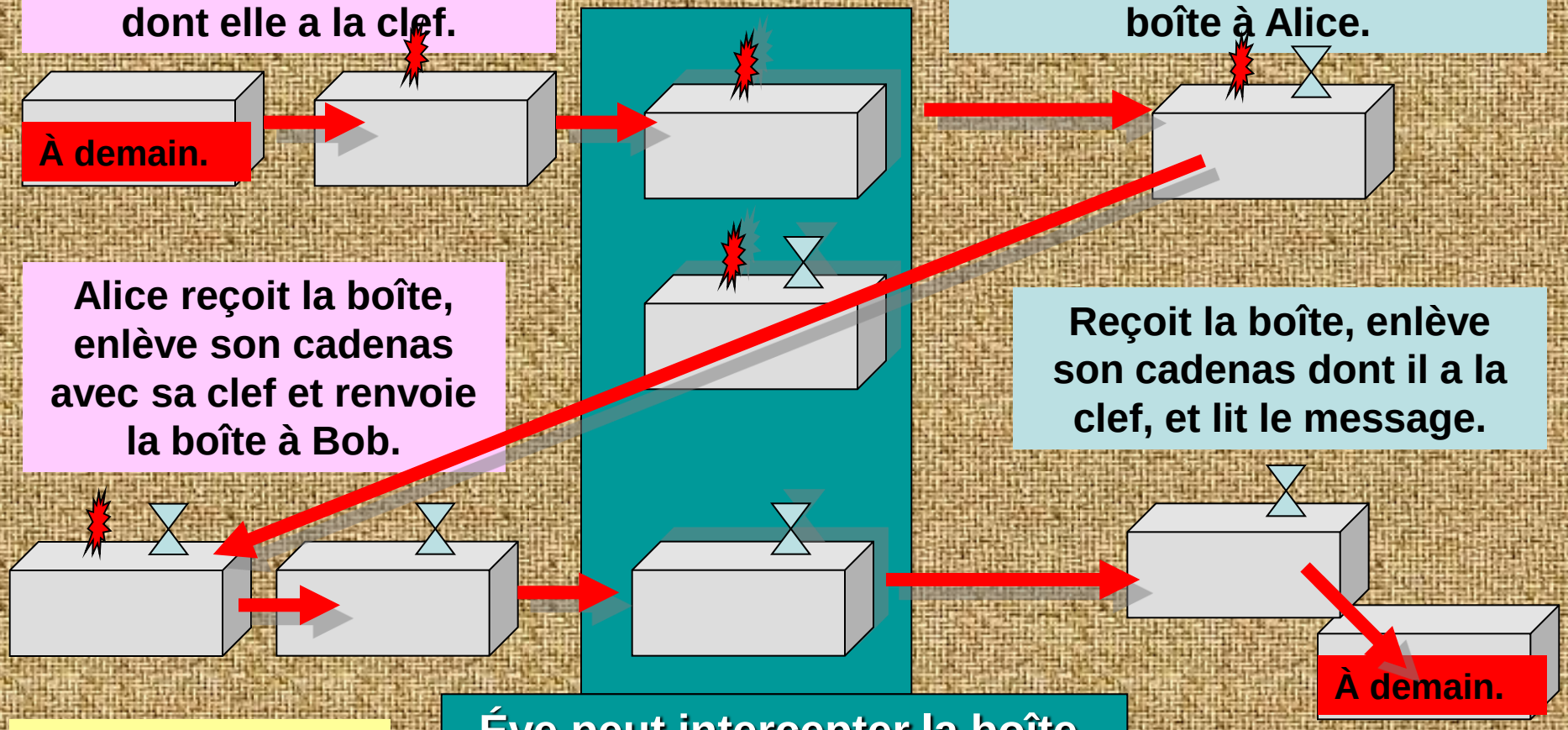
Cryptographie asymétrique:algorithme de Diffie-Hellman. 1976.

Alice

Bob

Met son message dans une boîte métallique fermée avec un cadenas dont elle a la clef.

Reçoit la boîte et sans l'ouvrir, met un cadenas dont il a la clef, puis renvoie la boîte à Alice.



Alice reçoit la boîte, enlève son cadenas avec sa clef et renvoie la boîte à Bob.

Reçoit la boîte, enlève son cadenas dont il a la clef, et lit le message.

Éve peut intercepter la boîte, mais ne peut l'ouvrir.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. p.100-103.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris. p. 315. p.321-324.

Cryptographie asymétrique: même clef secrète: Diffie-Hellman. 1976.

Alice (a) et Bob (b) décident par téléphone d'utiliser:

Le chiffre de mod doit être premier (>300 chiffres) et le (7) >100 chiffres.

Algorithme public.

$$f(x) \equiv 7^{x\,(\text{a ou b})} \pmod{11}$$

Alice (a) choisit en secret : 3

Bob (b) choisit en secret : 6

Chacun en secret calcule.

La cryptologie. P.Guillot. EDP Sciences 2013.p.47-48.

Alice(a=3): $7^3 \pmod{11} \equiv 2$ [343/11 reste 2]

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. p.100-103.

Bob (b=6): $7^6 \pmod{11} \equiv 4$ [117649/11 reste 4]

Par téléphone il échange leurs chiffres: 2 et 4.

Alice calcule $4^3 \equiv 64 \pmod{11} \equiv 9$.

Bob $2^6 \equiv 64 \pmod{11} \equiv 9$

$\equiv$

La clef est 9

Ils peuvent échanger des informations en DES (Data Encryption Standard) en toute sécurité.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.324-329-333.

Cryptographie asymétrique: chiffrement (clef publique)# déchiffrement(clef privée).

L'algorithme RSA (1977-2000 fin du brevet): Rivest, Shamir, Adelman.

Alice doit créer une clef (dite) publique.

N = p x q (nombres premiers).

N = 17 159 (secret) x 10 247 (secret) = 175 828 273 (public).

Alice choisit e de façon: e + (p-1)(q-1)= nombre premier.

e et N = clef publique.

Banque: $N > 10^{308}$

Bernard (et quiconque) pourra lui envoyer un message (M) chiffré (C) avec la clef publique (d'Alice).

Exemple (S.Singh p.472):

Clef publique d'Alice: N=187, e=7.

Message = ''X ''= 01011000 (en ASHII) = 88 (décimal). $C=88^7$ (mod 187)=11.

Alice reçoit les messages qu'elle décrypte avec sa clef privée: calcul de d

p=17, q=11, e=7. e x d = 1[mod(p-1)(q-1)]. d = 23.

$M = C^d$(mod 187). $M = 11^{23}$(mod 187). M = 88 =''X'' en ASHII

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. p.104-112. p.136.

La cryptologie. P.Guillot. EDP Sciences 2013.p.54-60.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.335-363; p.472-475.

Cryptographie asymétrique.

Systèmes à clef publique, clef privée.

Échange de clefs: <u>Diffie-Hellman</u> (1976)

Sac à dos: Hellman (1978). Cassé en peu de temps.

<u>RSA</u>: Rivest, Shamir, Adelman (1978). RSA-155 cassé en 1999. Solide avec des clefs plus longues que 155 chiffes.

Secte Aum Tokyo 1995 (S.Singh p381)

Ramsey Yousef : explosion du World Trade Center 26 février 1993. (S.Singh p381)

Courbes elliptiques: Miller, Koblitz (1985). Cartes à puces.

Le logiciel PGP: Pretty Good Privacy et Phil Zimmermann. 1991-….

PGP (Pretty Good Privacy): mélange de RSA et IDEA.

Phil Zimmermann et la NSA (1991)

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.p.365-396.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. p.107-108.

Initiation à la cryptographie. G. Dubertret. Édition Vuibert, Paris, 2012.p.155-156.

Le Monde 16 octobre 2013

‘’ ..le logiciel PGP…long et pénible….” ‘’Ansamb…à double clé…” ‘’nous ne stockerons pas les clés de chiffrement.” ‘’« Places » a besoin d’un annuaire centralisé… « distribué »..éclaté sur différents ordinateurs composant le réseau.”

2 | Le Monde Mercredi 16 octobre 2013 | SCIENCE & MÉDECINE | ACTUALITÉ

Tout crypter sans peine

INFORMATIQUE | Une start-up réunionnaise propose un système pour échanger textes, sons et images à l'abri des oreilles indiscrètes. Une offre qui arrive à point alors que les révélations se multiplient sur les écoutes gouvernementales

Yves Eudes

Tout crypter sans peine. Y. Eudes. Le Monde 16 octobre 2013. Science & Médecine. p.2.

(www.ansamb.com) (nom de code: « Places ») (Internet 3.O.)

à **10 Hz : λ = 34 mètres**

Les ondes mécaniques et l'air.

à **100 Hz : λ = 3,4 mètres** **λ= (vitesse du son dans l'air) 340 m/s / fréquence en Hertz.**

à **1000 Hz : λ = 0.34 mètres** **Diapason: (la) 440 Hz.**

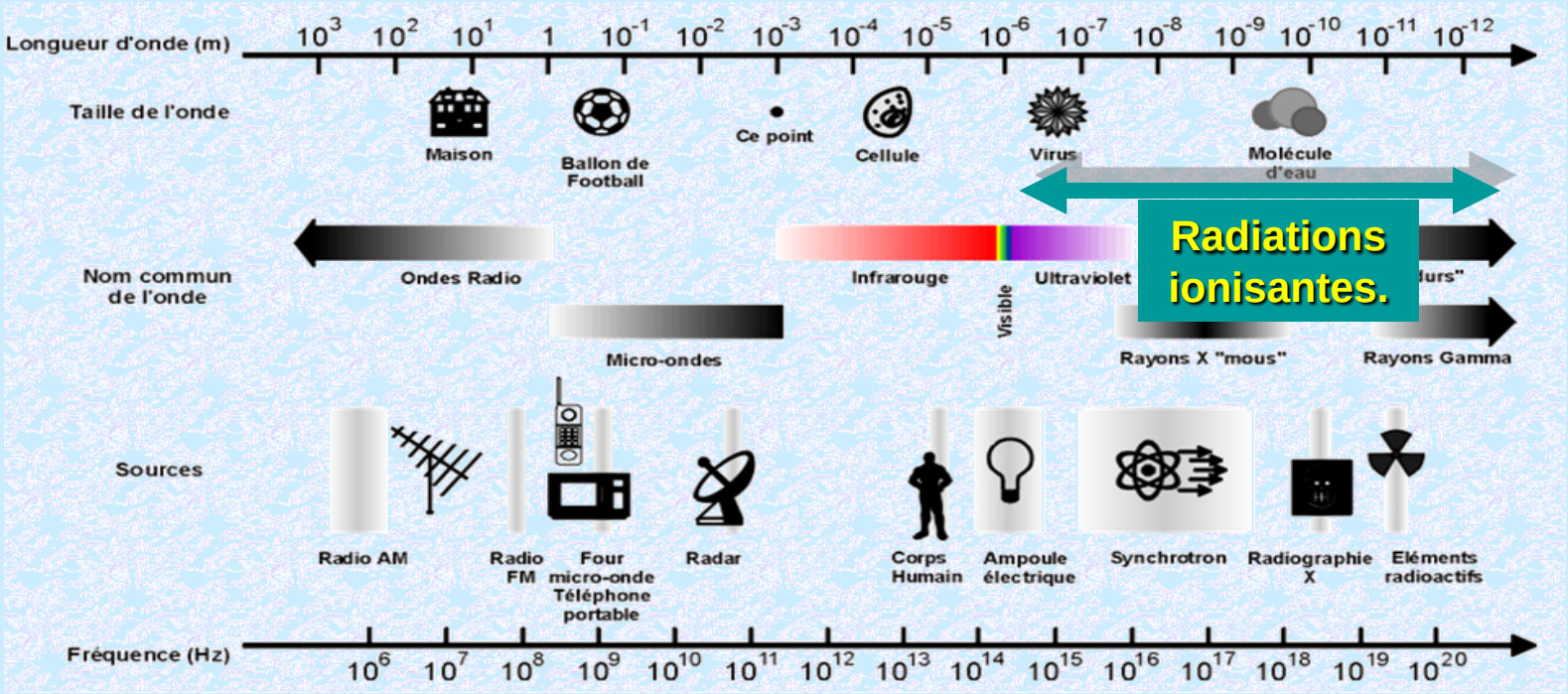
à **10 kHz : λ = 3,4 centimètre.** **Oreille perçoit: 20 Hz (grave) à 20 MHz (aigu).**

Les ondes électromagnétiques.

L'éclair et le tonnerre.

λ (en m) = (vitesse de la lumière) 300.10^6 m/s / fréquence en Hertz.

Les ondes électromagnétiques visibles: 380 nm (violet) – 780 nm (rouge).



Les ***ondes*** **hyperfréquences - *Polytech'Lille***

Hertz: 1oscillation par seconde (s-1 ou 1/s).

Désignation	Fréquence	Longueur d'onde	Exemples
Fréquences extrêmement basses (ELF)	0-300 Hz	10^5-10^3 km	Réseau électrique 50 Hz, électroménager…
Fréquences audio (VF)	0,3-3 kHz	1 000-100 km	Transmission de données vocales, métallurgie, chauffage par induction…
Très basses fréquences (VLF)	3-30 kHz	100-10 km	Radiocommunications…
Basses fréquences (LF)	30-300 kHz	10-1 km	Radiodiffusion GO, Fours à induction…
Fréquences moyennes (MF)	0,3-3 MHz	1 km-100 m	Radiodiffusion MO, PO, diathermie médicale…
Hautes fréquences (HF)	3-30 MHz	100-10 m	CB (citizen band), soudure, collage…
Très hautes fréquences (VHF)	30-300 MHz	10-1 m	Télévision, radio FM…
Fréquences ultrahautes (UHF)	0,3-3 GHz	1-0,1 m	Télévision, radars, téléphones mobiles, fours à micro-ondes, hyperthermie médicale…
Fréquences superhautes (SHF)	3-30 GHz	0,1-0,01 m	Radars, alarmes anti-intrusion
Fréquences extrêmement hautes (EHF)	30-300 GHz	0,01-0,001 m	Radars, communications par satellite, scanner corporel…
Infrarouge (IR)	0,3-385 THz	1 mm-780 nm	Spectrométrie IR, chauffage…
Lumière visible	385-750 THz	780-400 nm	Vision humaine, photosynthèse…
Ultraviolet (UV)	750 THz – 3 PHz	400-100 nm	Spectrométrie, lampes germicides, solarium…

Préfixes utilisés : k = kilo = 10^3 ; M = méga = 10^6 ; G = giga = 10^9 ; T = téra = 10^{12} ; P = péta = 10^{15} ; m = milli = 10^{-3} ; μ = micro = 10^{-6} ; n = nano = 10^{-9} ; GO : grandes ondes ; MO : ondes moyennes ; PO : petites ondes.

Champs électromagnétiques, environnement et santé. Sous la direction de A.Perrin, M.Souques. Édtions Springer-Verlag, Paris, 2011.p.11.

Ondes électromagnétiques

Production: sources naturelles, sources artificielles.

Propagation: Réflexion: miroir.

Réfraction: lors changement de milieu de propagation.

Diffusion: changement ou non de longueur d'onde.

Diffraction: sur un objet.

Interférences.

Interactions ondes et matières: Champ électrique, champ magnétique.
Champ proche, lointain.

Matériaux.

Matière vivante.

- **0 à 100 kHz**: Circulation de courants électriques: stimulation de tissus excitables.
- **100 kHz – 10 MHz**: échauffement des tissus et stimulation de tissus excitables.
- **> à 10 MHz**: échauffement des tissus.
- **3 PHz** (100 nm): Limite UV.

Ionisation.

Dose Absorption Spécifique (DAS).

Au cœur des ondes. Les champs électromagnétiques en question. F. Ndagijimana, F.Gaudaire. Éditions Dunod, Paris, 2013.p.138-140.

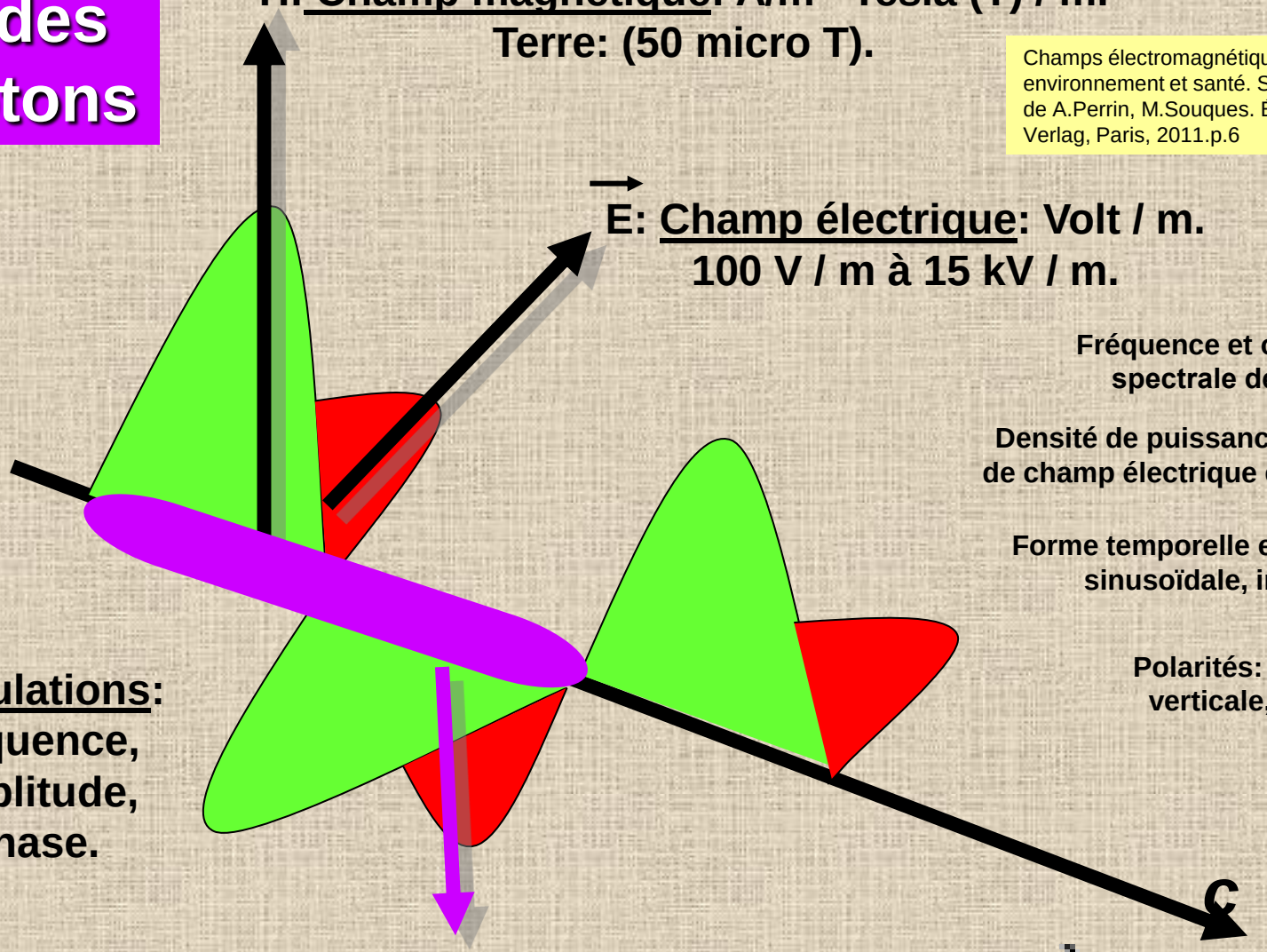
Champs électromagnétiques, environnement et santé. Sous la direction de A.Perrin, M.Souques. Édtions Springer-Verlag, Paris, 2011.p.8-10.

Ondes Photons

$\vec{H}$: Champ magnétique: A/m Tesla (T) / m.
Terre: (50 micro T).

Champs électromagnétiques, environnement et santé. Sous la direction de A.Perrin, M.Souques. Édtions Springer-Verlag, Paris, 2011.p.6

$\vec{E}$: Champ électrique: Volt / m.
100 V / m à 15 kV / m.



Fréquence et occupation spectrale de l'onde.

Densité de puissance: amplitudes de champ électrique et magnétique.

Forme temporelle et fréquentielle: sinusoïdale, impulsion.

Polarités: horizontale, verticale, circulaire.

Modulations: fréquence, amplitude, phase.

Directions.

Polarités.

Longueur d'onde (m.s.) (lambda) $\lambda = \frac{c}{f}$

c = vitesse de la lumière: 299 792 458 m/s

f = fréquence (1 cycle par seconde)(Hertz / s).

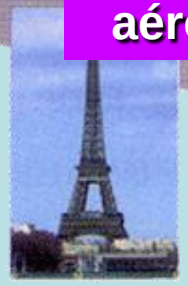
50 Hz | 10^5 Hz | 10^{10} Hz | 10^{14} Hz | 10^{20} Hz | 10^{22} Hz

20.10^6 Hz: aéroport.

Visible: de 750 à 385 THz

Visible: de 400 à 780 nm

Visible: de 3,1 à 1,59 eV



Champs électromagnétiques, environnement et santé. Sous la direction de A.Perrin, M.Souques. Édtions Springer-Verlag, Paris, 2011.p.12.

Radiations non ionisantes | Radiations ionisantes

$1,24.10^{-11}$ eV | $1,24.10^{-6}$ eV | 0,3 eV | >12,4 eV | $2,48.10^6$ eV

10^3 m. | 1 m. | Seuil: 13,6 eV. | 10^{-12}m.

Ondes électromagnétiques et le Vivant.

Effets fonctionnels:

Niveaux: moléculaires, cellulaires,…

Effets structurels:

Non pathologiques, Pathologiques provisoires, définitifs,…

Les Photosynthèses:

Chlorophylle: bleu (vers 430 nm), rouge (vers 660 nm).

Phycobilines: cyanobactéries, algues rouges.

Caroténoïdes: bleu-vert (460nm- 520nm).

Photosynthèse oxygénique.

Plantes supérieures terrestres, algues, cyanobactéries.

$$6\ CO_2 + 12\ H_2O + \text{lumière} >>>>> C_6H_{12}O_6 + 6\ O_2 + 6\ H_2O.$$

C + énergie photonique >>>>> C excité + électron.

$$2\ H_2O >>>>> 4\ H^+ + 4\ e^- + O_2$$

Électron photosynthétique dans chaîne réactionnelle. Synthèse d'ATP.

Photosynthèse anoxygénique: bactéries pourpres, vertes.

Bactéries sulfureuses, non sulfureuses.

Effets de forts éclairements:

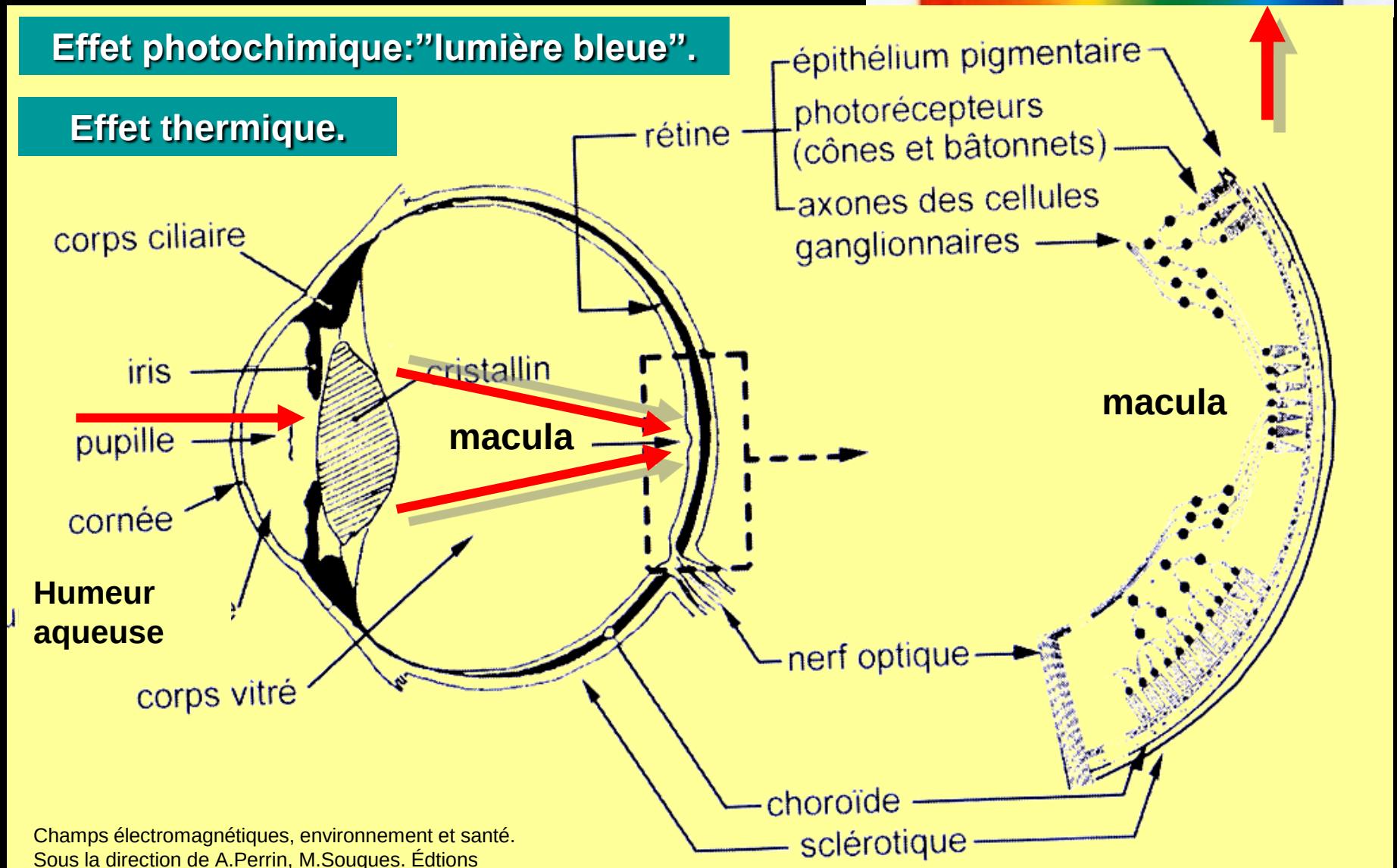
Inhibition de la photosynthèse. Stress oxydatif. (p.346-351)

La photosynthèse. J. Farineau, JF. Morot-Gaudry. INRA, Paris, 2006.p.28, 40, 47- 57, 155, ,202, 217, 231.

Œil : ondes électromagnétiques photoniques.

Effet photochimique:"lumière bleue".

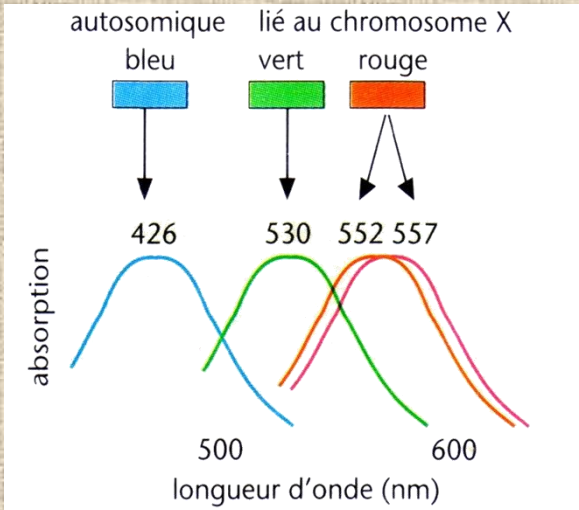
Effet thermique.



Champs électromagnétiques, environnement et santé. Sous la direction de A.Perrin, M.Souques. Édtions Springer-Verlag, Paris, 2011.p.103-114.

Œil: rétine.

Sensible de 380nm à 780nm



A. Gènes codant les protéines photo-réceptrices localisées dans les cônes

Atlas de Génétique. E.Passarge. Éditions Médecine-Sciences, Flammarion, Paris, 2003.p.283.

1) Cônes: opsines (+ rétinal): (macula +++): vision colorée diurne. color vision

Rouge (800-620nm)(375-483THz): Xq28.

Vert (570-490nm)(526-612THz): Xq28.

Bleu (490- 485nm)(612-619THz)(macula: 0): autosomique: 7q32.1

Achromatopsie: absence de cônes.

Tritanopie: perte vision du bleu. 190900

Daltonismes: vert, rouge, vert et rouge.

2) Bâtonnets (macula: 0): rhodopsine (+rétinal): vision crépusculaire: intensité lumineuse (510 nm): 3q21-24.

mutations: rétinites pigmentaires.

3) Cellules ganglionnaires (mélanopsine)(480nm): glande pinéale (mélatonine) (photopériode): rythme circadien automatique et nycthéméral

''rétinien''; durée de la nuit; flash; réflexe photosexuel.

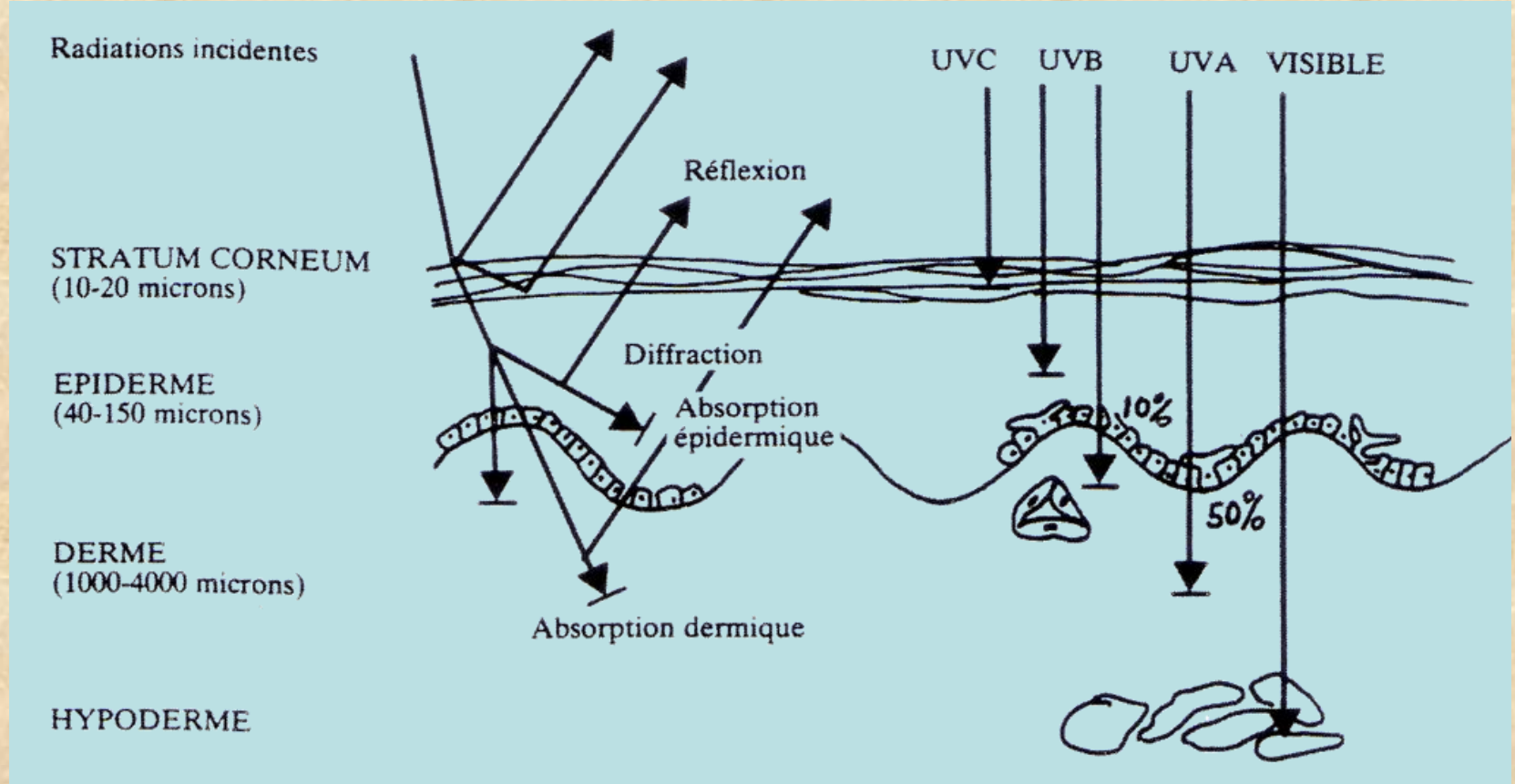
4) Les magnétophosphènes: < 10 kH.

Champs électromagnétiques, environnement et santé. Sous la direction de A.Perrin, M.Souques. Édtions Springer-Verlag, Paris, 2011.p.60.

5) Récepteurs extraoculaires:?

Environnement et rythmes de reproduction. B. Mapaux. *in* La reproduction chez les Mammifères et l'Homme. C.Thibault, M.C.Levasseur. Éditions Ellipses, Paris, 2001.p.699-718.

Peau: ondes électromagnétiques.



Bilirubine (lumière bleue).

Vita. D: UVB.

Phototoxicité.

Mélanocytes: UVA+.

Radiodermite.

Photosensibilité.

Érythème actinique:UVB+(308nm).

Génophotodermatoses.

Champs électromagnétiques, environnement et santé. Sous la direction de A.Perrin, M.Souques. Édtions Springer-Verlag, Paris, 2011.p.121.

Apport de l'étude de l'excision-réparation de l'ADN au diagnostic des génodermatoses. F.Vasseur,….Nouv.Dermatol. 9,5,424-430,1990.

Conclusions.

Le principe de A. Kerckhoffs (1883) et son actualité.

‘’la sécurité d’un système de cryptement ne doit pas dépendre de la préservation du secret de l’algorithme. Le secret ne repose que sur le secret de la clef.”

La place de la technologie.

À propos du Système R.I.T.A.

Transmissions dans l'armée française - Wikipédia

LE RÉSEAU INTÉGRÉ DE TRANSMISSIONS AUTOMATIQUE

Réseau intégré des transmissions automatiques - Wikipédia

L'univers des codes secrets. H.Lehning. Ixelles, Publishing SA, 2012. p.20.

Le livre des Codes. Sélection du Reader's Digest. Bagneux, 2009. p.65.

Codage et cryptographie. J.Gomez. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. Tome 2.

Du boulier à la révolution numérique. V. Torra. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. Tome 13.

Les nombres premiers. E.Gracian. Collection ''Le Monde est Mathématique'' éditée par RBA France, SARL, Paris. 2013. Tome 3.

Initiation à la cryptographie. G. Dubertret. Édition Vuibert, Paris, 2012.

La photosynthèse. J. Farineau, JF. Morot-Gaudry. INRA, Paris, 2006.p.28, 40, 47- 57, 155, ,202, 217, 231.

Histoire des codes secrets. S.Singh. Éditions Jean-Claude Lattès, 1999, Paris.

Les codes secrets décryptés. D.Müller. City Editions 2007.

Le secret de la Grande Guerre. Barbara Tuchman. Librairie Arthème Fayard, Paris, 1965.

Le grand livre des codes secrets. M. Piquemal, D. Royo. Illustrations C. Dutertre. Albin Michel Jeunesse, Paris, 2004.

Introduction à la cyberstratégie. O. Kempf. Éditions Economica, Paris, 2012. p.21.

Le radio-amateur. Olivier Pilloud. Éditions Technip, Paris, 2007. 3ème édition.

Les casseurs de codes (de la seconde guerre mondiale). Sinclair McKay. Éditions, Ixelles Publishing SA, 2012.

La cryptologie. P.Guillot. EDP Sciences 2013.

Champs électromagnétiques, environnement et santé. Sous la direction de A.Perrin, M.Souques. Édtions Springer-Verlag, Paris, 2011.

Au cœur des ondes. Les champs électromagnétiques en question. F. Ndagijimana, F.Gaudaire. Éditions Dunod, Paris, 2013.

Des trains d'ondes dans les habitations. D.Viandier Francru. Éditions Ellipses, Paris, 2013.

La place de l'homme dans la nature. P.Teilhard de Chardin. Éditions Albin Michel, Paris,1956. (p.111).

Environnement et rythmes de reproduction. B. Mapaux. *in* La reproduction chez les Mammifères et l'Homme. C.Thibault, M.C.Levasseur. Éditions Ellipses, Paris, 2001.p.699-718.

Atlas de Génétique. E.Passarge. Éditions Médecine-Sciences, Flammarion, Paris, 2003.p.283.