Cryptographie

Définition :
Du grec kryptos (caché) et graphein (écriture). La cryptographie est l'art de modifier un message jusqu'à le rendre incompréhensible pour ceux à qui il n'est pas destiné. Plus généralement, c'est l'art d'exprimer secrètement ses sentiments et ses pensées, par des mots obscurs, par des écrits équivoques ou par des mouvements et des signes.(Littré)
La cryptographie comprend de nombreuses méthodes dont la principale est la substitution (échanger les lettres par d'autres signes). Une méthode de substitution est appelée un chiffre.

Liste des mini projets

Pour chaque mini projet, vous devrez élaborer

Cryptage :
1. Un brouillon de présentation visuelle de l'algorithme de cryptage sur une feuille A3.
2. L'algorithme de cryptage en Javascript (et EnyoJS pour l'interface)

Décryptage :
3. Un brouillon de présentation visuelle de l'algorithme de décryptage sur une feuille A3.
4. L'algorithme de décryptage en Javascript (et EnyoJS pour l'interface)

5. Un diaporama expliquant cet algorithme et son contexte historique. (support de votre présentation orale)

Projet	Difficulté	Les indices proposés sur **picassciences.com**
Méthode de César		Vidéo CESAR
Méthode de Vigenère		Vidéo CESAR Vidéo VIGENERE
La machine Enigma		Vidéo CESAR Vidéo ENIGMA Vidéo ENIGMA INFOS ADDITIONNELLES

Chaque projet dispose d'un répertoire de fichier proposé par le professeur contenant des indices. Vous pourrez une fois le travail effectué vous envoyer des messages codés à vos camarades.

Prérequis :

Vous aurez besoin **du cours sur les tableau** en Javascript afin de définir les textes à crypter et les clés de cryptage.

Information supplémentaire :
Une chaine de caractère TEXTE = « BONJOUR » est en fait un tableau dont chaque case est remplie par une lettre. Ainsi pour accéder à une lettre de cette chaine, on utilisera la commande suivante :
A = TEXTE[2] // ce qui revoie la lettre N

Cryptographie – éléments de résolution

I. La table ASCII :

Hex	Dec	Char		Hex	Dec	Char		Hex	Dec	Char		Hex	Dec	Char	
0x00	0	NULL	null	0x20	32	Space		0x40	64	@		0x60	96	`	
0x01	1	SOH	Start of heading	0x21	33	!		0x41	65	A		0x61	97	a	
0x02	2	STX	Start of text	0x22	34	"		0x42	66	B		0x62	98	b	
0x03	3	ETX	End of text	0x23	35	#		0x43	67	C		0x63	99	c	
0x04	4	EOT	End of transmission	0x24	36	$		0x44	68	D		0x64	100	d	
0x05	5	ENQ	Enquiry	0x25	37	%		0x45	69	E		0x65	101	e	
0x06	6	ACK	Acknowledge	0x26	38	&		0x46	70	F		0x66	102	f	
0x07	7	BELL	Bell	0x27	39	'		0x47	71	G		0x67	103	g	
0x08	8	BS	Backspace	0x28	40	(		0x48	72	H		0x68	104	h	
0x09	9	TAB	Horizontal tab	0x29	41	)		0x49	73	I		0x69	105	i	
0x0A	10	LF	New line	0x2A	42	*		0x4A	74	J		0x6A	106	j	
0x0B	11	VT	Vertical tab	0x2B	43	+		0x4B	75	K		0x6B	107	k	
0x0C	12	FF	Form Feed	0x2C	44	,		0x4C	76	L		0x6C	108	l	
0x0D	13	CR	Carriage return	0x2D	45	-		0x4D	77	M		0x6D	109	m	
0x0E	14	SO	Shift out	0x2E	46	.		0x4E	78	N		0x6E	110	n	
0x0F	15	SI	Shift in	0x2F	47	/		0x4F	79	O		0x6F	111	o	
0x10	16	DLE	Data link escape	0x30	48	0		0x50	80	P		0x70	112	p	
0x11	17	DC1	Device control 1	0x31	49	1		0x51	81	Q		0x71	113	q	
0x12	18	DC2	Device control 2	0x32	50	2		0x52	82	R		0x72	114	r	
0x13	19	DC3	Device control 3	0x33	51	3		0x53	83	S		0x73	115	s	
0x14	20	DC4	Device control 4	0x34	52	4		0x54	84	T		0x74	116	t	
0x15	21	NAK	Negative ack	0x35	53	5		0x55	85	U		0x75	117	u	
0x16	22	SYN	Synchronous idle	0x36	54	6		0x56	86	V		0x76	118	v	
0x17	23	ETB	End transmission block	0x37	55	7		0x57	87	W		0x77	119	w	
0x18	24	CAN	Cancel	0x38	56	8		0x58	88	X		0x78	120	x	
0x19	25	EM	End of medium	0x39	57	9		0x59	89	Y		0x79	121	y	
0x1A	26	SUB	Substitute	0x3A	58	:		0x5A	90	Z		0x7A	122	z	
0x1B	27	FSC	Escape	0x3B	59	;		0x5B	91	[		0x7B	123	{	
0x1C	28	FS	File separator	0x3C	60	<		0x5C	92	\		0x7C	124	|	
0x1D	29	GS	Group separator	0x3D	61	=		0x5D	93	]		0x7D	125	}	
0x1E	30	RS	Record separator	0x3E	62	>		0x5E	94	^		0x7E	126	~	
0x1F	31	US	Unit separator	0x3F	63	?		0x5F	95	_		0x7F	127	DEL	

L'American Standard Code for Information Interchange (Code américain normalisé pour l'échange d'information), plus connu sous l'acronyme ASCII est une norme de codage de caractères en informatique ancienne et connue pour son influence incontournable sur les codages de caractères qui lui ont succédé. Elle était la plus largement compatible pour ce qui est des caractères latins non accentués.
Afin de coder chaque caractère, ces derniers sont associés à des numéros selon l'ordre suivant : (voir à gauche)

II. Table ASCII et cryptographie :

Afin de pouvoir transformer rapidement des lettres en nombres dans le cas de méthode de cryptage comme César, Vigenère, Enigma, etc… on peut utiliser les fonctions suivantes :

- Méthode **charCodeAt** : Convertir une lettre en nombre :

  chaine = "HELLO WORLD";

  a = chaine.charCodeAt(0); // Extrait la première lettre de la chaine de caractères.

  Le résultat a va être : 72

  Plus d'infos sur : http://www.w3schools.com/jsref/jsref_charCodeAt.asp

- Méthode **fromCharCode** : Convertir un nombre en lettre :

  a = String.fromCharCode(65);

  Le résultat a va être : « A »

  Plus d'infos sur : http://www.w3schools.com/jsref/jsref_fromCharCode.asp

NOTE : des indices supplémentaires se trouvent dans le code de départ.