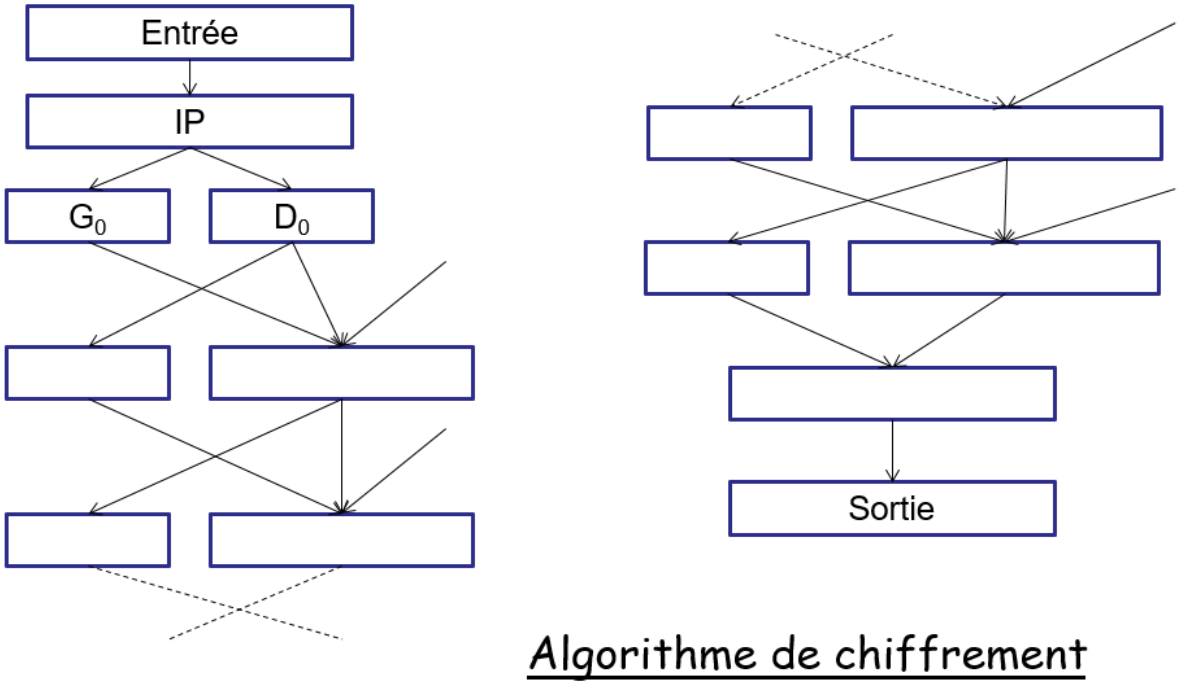
Durée : 1h30 Le 24/06/2020

CONTROLE FINAL
CHIFFREMENT AUDIO

Questions de cours (5 pts)

1. Comment assurer une transmission de données audio rapide et protégée ?
2. La banque de filtres de l'algorithme MP3 est utilisée pour diviser le signal d'entrée en combien de sous-bandes ?
3. Compléter l'organigramme de l'algorithme de chiffrement DES suivant :



Algorithme de chiffrement

4. Quelle est la taille de la clé de l'algorithme Shuffle ?

Problème (15 pts)

Soit l'algorithme de l'expansion permet de générer le (Key Schedule) à utiliser dans les différents tours de l'algorithme de chiffrement audio utilisant AES (Advanced Encryption Standard). Cet algorithme permet de générer des sous-clés de 128 bits chacune à partir d'une clé de chiffrement de 128 bits.

Utilisez cet algorithme pour calculer la première sous-clés (K_1) générée à partir de la clé de chiffrement suivante :

K = 01 23 45 67 89 AB CD EF 01 23 45 67 89 AB CD EF

Annexe :

Table RCon :

2^i	01	02	04	08	10	20	40	80	1b	36
0	00	00	00	00	00	00	00	00	00	00
0	00	00	00	00	00	00	00	00	00	00
0	00	00	00	00	00	00	00	00	00	00

Table S-Box :

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Bonne chance…

NB: Le corrigé type est disponible sur le site : http://www.larbiguezouli.com

CORRECTION DU CONTROLE FINAL
CHIFFREMENT AUDIO

Questions de cours (5 pts)

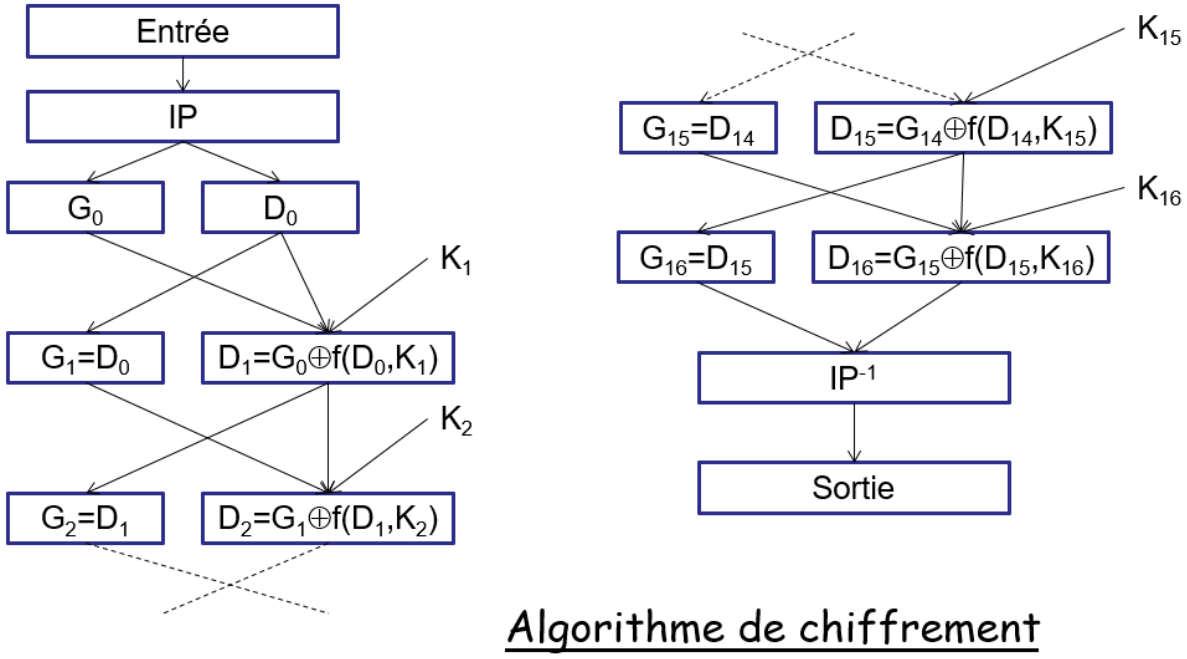
1. Comment assurer une transmission de données audio rapide et protégée ? (1 pt)

Pour assurer une transmission de données audio rapide et protégée il faut **compresser les données** pour réduire la taille et la transmission sera rapide, et il faut **chiffrer les données** pour les protéger.

2. La banque de filtres de l'algorithme MP3 est utilisée pour diviser le signal d'entrée en combien de sous-bandes ? (1 pt)

La banque de filtres de l'algorithme MP3 est utilisée pour diviser le signal d'entrée en **32 sous-bandes**.

3. Compléter l'organigramme de l'algorithme de chiffrement DES suivant : (2 pts)



Algorithme de chiffrement

4. Quelle est la taille de la clé de l'algorithme Shuffle ? (1 pt)

La clé de l'algorithme Shuffe **n'a pas de taille fixe**, on peut lui donner n'importe quelle taille.

Problème (15 pts)

Soit l'algorithme de l'expansion permet de générer le (Key Schedule) à utiliser dans les différents tours de l'algorithme de chiffrement audio utilisant AES (Advanced Encryption Standard). Cet algorithme permet de générer des sous-clés de 128 bits chacune à partir d'une clé de chiffrement de 128 bits.

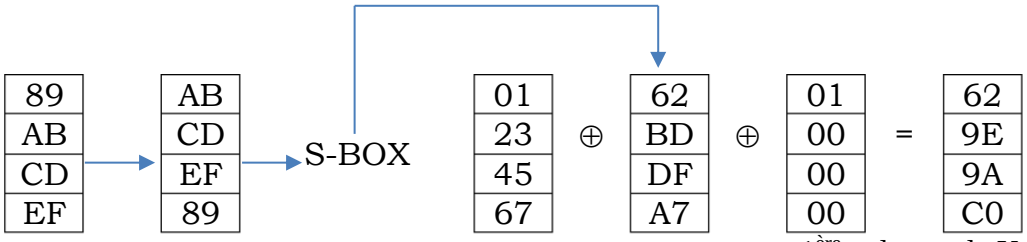
Utilisez cet algorithme pour calculer la première sous-clés (K_1) générée à partir de la clé de chiffrement suivante :

K = 01 23 45 67 89 AB CD EF 01 23 45 67 89 AB CD EF

- Récupérer la clé de chiffrement **K** sous forme de 4 colonnes de 4 octets chacune. (1 pt)

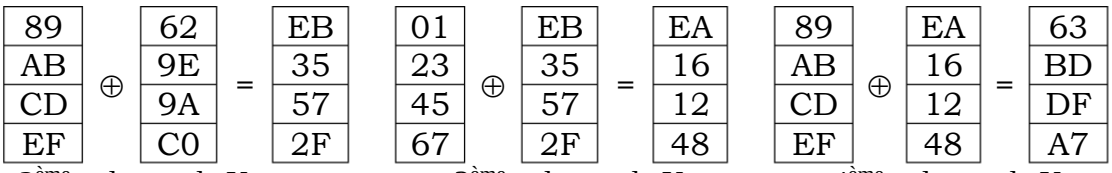
01	89	01	89
23	AB	23	AB
45	CD	45	CD
67	EF	67	EF

- Pour construire la 1ère colonne de la clé $\mathbf{K_1}$ du **tour$_1$**, on utilise la 4ème colonne de la clé K, on fait une **rotation** vers le haut de 1 octet, puis on applique une transformation en utilisant la table **S-Box**, puis on applique le **XOR** entre la 1ère colonne de K, la colonne transformée et la 1ère colonne de Rcon. (7 pts)



1ère colonne de K_1

- Pour construire les 2ème, 3ème et 4ème colonnes de la clé $\mathbf{K_1}$ du **tour$_1$**, on fait le **XOR** respectivement de la 2ème colonne de K avec la 1ère colonne de K_1, la 3ème colonne de K avec la 2ème colonne de K_1 et la 4ème colonne de K avec la 3ème colonne de K_1 : (7 pts)



2ème colonne de K_1 3ème colonne de K_1 4ème colonne de K_1

62	EB	EA	63
9E	35	16	BD
9A	57	12	DF
C0	2F	48	A7

La sous-clé K_1