Contrôle continu – Cryptographie et sécurité

Attention : vous devrez rendre ce sujet avec votre copie

Questions de cours *(5 pts)*

Dans toutes les questions ci-dessous, nous attendons des réponses claires, précises et personnelles.

1. Nous avons une image de 3870 pixels par 7600 pixels. Nous voulons cacher une donnée sur le bit de poids faible de chaque composante de couleur (en partant du principe qu'on est en RGB sans canal alpha). Pour rappel, nous avons besoin de trois octets qui coderont la taille de la donnée à cacher. Quelle taille maximale peut avoir cette donnée pour que la stéganographie soit possible selon la méthodologie vue en TP ? *(1.5 pt)*
2. D'ailleurs, en quoi est-ce utile d'enregistrer la taille de la donnée cachée ? *(1 pt)*
3. Soit **o** une variable stockant un octet (représenté sous la forme d'un entier entre 0 et 255). Soit **d** la donnée de 2 bits « **10** ». Donnez, en Python, les lignes de code qui permettront de remplacer les deux bits de poids faible de **o** par la donnée **d**. *(1.5 pt)*
4. En quoi l'indice de coïncidence est-il utile dans la cryptanalyse de Vigenère ? *(1 pt)*

Exercice 1 *(7 pts)*

1. Donnez précisément les schémas du CTR en chiffrement et en déchiffrement. *(1 pt)*
2. Nous avons intercepté l'échange suivant. Visiblement il y a du CTR dans l'air, et on fonctionne avec un mini-AES et des blocs de 16 bits. On sait de source sûre que le premier message de Yoh est : « `Mat Mat!` » (sans les guillemets ni les espaces associés aux guillemets). On sait aussi que le second message clair de Yoh et le premier message clair de Mathieu sont identiques à 100 %.
   a. Détaillez précisément la méthodologie qui vous permettra de déchiffrer l'intégralité de cette discussion. *(3 pts)*
   b. Déchiffrez le dernier message envoyé par Mat. Tous les calculs doivent apparaître sur votre copie. Aucune réponse magique sortant du chapeau ne sera considérée. Ne soyez pas surpris par une incohérence apparente des messages déchiffrés. *(2 pts)*

   1. `Yoh:24ae 4d8a 64cd b5f0 bcb1`
   2. `Yoh:24ae 31d9 68dc cbae`
   3. `Mat:bf24 3e86 f781 dc8a`
   4. `Mat:bf24 3294 bb82`
   5. `Yoh:24ae 4d8e 628e 91b0`
3. Normalement, vous avez désormais toutes les billes en main pour envoyer un message à Yoh, en vous faisant passer pour Mat. Avec la configuration CTR de Mat, chiffrez les 4 octets du message suivant : « `Top!` » *(1 pt)*

Exercice 2 *(8 pts)*

Le message suivant a été chiffré avec un chiffrement similaire à Vigenère, mais où le décalage alphabétique est remplacé par une opération XOR entre l'octet courant et l'octet de la clé. L'opération XOR a été réalisée sur les codes ASCII des caractères. Le message chiffré obtenu contient donc des valeurs hexadécimales.

Le message initial en clair contient uniquement des lettres capitales non accentuées. Il ne contient donc aucune lettre minuscule ou chiffre, aucun caractère spécial, aucun espace ou ponctuation, et aucun caractère codé sur plus d'un octet.

Voici le texte chiffré :

```
21 23 35 3b 3b 39 26 3b 35 3a 2a 23 3b 2e 3e 3c 2b 35
3b 2a 20 24 20 3e 2f 2a 22 2c 2e 3e 3b 23 35 2b 27 39
2e 29 22 2d 22 35 26 3b 20 27 23 29 29 23 20 20 2e 32
…(648 octets)…
25 22 31 3a 26 21 3d 2a 24 29 23 31 20 20 25 38 3f 35
24 2e 22 2d 3f 3f 26 3c 35 29 2b 3f 26 21 35 3a 2a 23
3c 28 3f 23 3a
```

Comme il s'agit d'un chiffrement similaire à Vigenère, on s'est dit qu'il fallait créer des sous-textes et dénombrer le occurrences (nombre d'apparitions) de chaque octet dans chaque sous-texte.

Le tableau page suivante détaille les occurrences obtenues pour plusieurs longueurs de clé supposées.

1. Détaillez la marche à suivre pour déchiffrer le message à partir du tableau des occurrences. *(3 pts)*
2. Donnez la clé de chiffrement que vous aurez trouvée à partir des éléments donnés. *(3 pts)*
3. Déchiffrez les *4 premiers* et les *4 derniers* octets du message chiffré. *(2 pts)*

Question bonus

Sur quelle composante était cachée le message dans la première image du pdf du cours ?

Taille supposée de la clé	Numéro de sous-texte	Nb octets du texte	Nombre d'occurrences de chaque octet
1	1	743	20→25 | 21→42 | 22→26 | 23→34 | 24→28 | 25→31 | 26→47 | 27→14 28→3 | 29→29 | 2a→40 | 2b→19 | 2c→17 | 2d→39 | 2e→29 | 2f→2 30→1 | 31→20 | 32→1 | 33→5 | 34→4 | 35→35 | 36→5 | 37→2 38→9 | 39→37 | 3a→26 | 3b→40 | 3c→43 | 3d→35 | 3e→30 | 3f→25
2	1	372	20→17 | 21→19 | 22→18 | 23→9 | 24→13 | 25→12 | 26→27 | 27→6 29→13 | 2a→18 | 2b→13 | 2c→10 | 2d→16 | 2e→9 | 2f→2 | 31→12 33→2 | 34→2 | 35→19 | 36→2 | 37→2 | 38→6 | 39→17 | 3a→11 3b→21 | 3c→25 | 3d→19 | 3e→19 | 3f→13
	2	371	20→8 | 21→23 | 22→8 | 23→25 | 24→15 | 25→19 | 26→20 | 27→8 28→3 | 29→16 | 2a→22 | 2b→6 | 2c→7 | 2d→23 | 2e→20 | 30→1 31→8 | 32→1 | 33→3 | 34→2 | 35→16 | 36→3 | 38→3 | 39→20 3a→15 | 3b→19 | 3c→18 | 3d→16 | 3e→11 | 3f→12
3	1	248	20→2 | 21→24 | 22→2 | 23→1 | 24→14 | 25→7 | 26→18 | 27→11 29→23 | 2b→8 | 2c→10 | 2d→37 | 2e→3 | 2f→2 | 30→1 | 38→6 39→8 | 3a→9 | 3b→21 | 3c→20 | 3d→17 | 3e→4
	2	248	20→16 | 21→14 | 22→7 | 23→16 | 25→2 | 26→21 | 27→3 | 28→3 29→5 | 2a→40 | 2b→11 | 2c→7 | 2d→2 | 2e→26 | 37→2 | 39→3 3a→17 | 3b→19 | 3c→8 | 3d→12 | 3e→5 | 3f→9
	3	247	20→7 | 21→4 | 22→17 | 23→17 | 24→14 | 25→22 | 26→8 | 29→1 31→20 | 32→1 | 33→5 | 34→4 | 35→35 | 36→5 | 38→3 | 39→26 3c→15 | 3d→6 | 3e→21 | 3f→16
4	1	186	20→7 | 21→11 | 22→8 | 23→4 | 24→6 | 25→8 | 26→13 | 27→1 29→8 | 2a→10 | 2b→8 | 2c→5 | 2d→4 | 2e→4 | 2f→2 | 31→5 34→1 | 35→10 | 36→1 | 37→2 | 38→2 | 39→7 | 3a→7 | 3b→7 3c→18 | 3d→13 | 3e→8 | 3f→6
	2	186	20→3 | 21→11 | 22→4 | 23→16 | 24→11 | 25→6 | 26→5 | 27→4 28→1 | 29→8 | 2a→13 | 2b→4 | 2c→4 | 2d→11 | 2e→12 | 30→1 31→4 | 32→1 | 33→2 | 34→1 | 35→9 | 36→1 | 38→1 | 39→9 3a→7 | 3b→7 | 3c→8 | 3d→10 | 3e→5 | 3f→7
	3	186	20→10 | 21→8 | 22→10 | 23→5 | 24→7 | 25→4 | 26→14 | 27→5 29→5 | 2a→8 | 2b→5 | 2c→5 | 2d→12 | 2e→5 | 31→7 | 33→2 34→1 | 35→9 | 36→1 | 38→4 | 39→10 | 3a→4 | 3b→14 | 3c→7 3d→6 | 3e→11 | 3f→7
	4	185	20→5 | 21→12 | 22→4 | 23→9 | 24→4 | 25→13 | 26→15 | 27→4 28→2 | 29→8 | 2a→9 | 2b→2 | 2c→3 | 2d→12 | 2e→8 | 31→4 33→1 | 34→1 | 35→7 | 36→2 | 38→2 | 39→11 | 3a→8 | 3b→12 3c→10 | 3d→6 | 3e→6 | 3f→5

La notation « X→Y » signifie que l'octet X (en hexadécimal) apparaît Y fois dans le sous-texte chiffré.

Annexes

Table ASCII

Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char
20	*espace*	30	0	40	@	50	P	60	`	70	p
21	!	31	1	41	A	51	Q	61	a	71	q
22	"	32	2	42	B	52	R	62	b	72	r
23	#	33	3	43	C	53	S	63	c	73	s
24	$	34	4	44	D	54	T	64	d	74	t
25	%	35	5	45	E	55	U	65	e	75	u
26	&	36	6	46	F	56	V	66	f	76	v
27	'	37	7	47	G	57	W	67	g	77	w
28	(	38	8	48	H	58	X	68	h	78	x
29	)	39	9	49	I	59	Y	69	i	79	y
2A	*	3A	:	4A	J	5A	Z	6A	j	7A	z
2B	+	3B	;	4B	K	5B	[	6B	k	7B	{
2C	,	3C	<	4C	L	5C	\	6C	l	7C	|
2D	-	3D	=	4D	M	5D	]	6D	m	7D	}
2E	.	3E	>	4E	N	5E	^	6E	n	7E	~
2F	/	3F	?	4F	O	5F	_	6F	o		

Opération XOR « X ^ Y » entre deux valeurs hexadécimales « X » et « Y »

XOR	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0