M1 informatique/MIAGE **Univ. Orléans**
CRYPTO **2023-2024**

Contrôle terminal – session 2

Les calculatrices autorisées sont celles dont le modèle est inférieur ou équivalent à une calculatrice collège.
Il y a 4 points bonus dans ce sujet.
Sujet à rendre avec votre copie.

Ex1. Du classique CTR - 6 pts

Dans le Discord des étudiants, un étudiant a diffusé ce qu'il a réussi à récupérer. Ce sont les mots de passe chiffrés des professeurs de cryptographie. On sait juste que le mot de passe de Mathieu Chapelle est : tata#1. C'est bien beau, mais ça n'aide pas pour se connecter au compte de Yohan BOICHUT ou de Maël DUMAS.

1. Yohan BOICHUT : `076c 708b 508d 92ce`
2. Mathieu CHAPELLE : `076c 709f 5099 97cc`
3. Maël DUMAS : `076c 749f 5499 90cc`

Questions

1. Appliquez vos connaissances pour extraire les deux mots de passe manquants. Détaillez vos calculs.
2. Ajoutez une nouvelle entrée en chiffrant le mot de passe **thks!!** pour faire croire que Bob est aussi dans le système d'information. Il faut alors que le mot de passe soit chiffré de la même façon que les trois autres.

Ex2. Stéganographie - 6 points

Nous avons récupéré un extrait d'image (une séquence de pixels RGB). Il est caché dans cette image un mot de trois lettres suivant l'algorithme *LSB*. Toutes les composantes couleurs contiennent un seul bit du mot mystère. Pour rappel, un caractère = un octet.

id pixel	0	1	2	3
Pixel	(108, 231, 69)	(79, 0, 120)	(170, 148, 4)	(167, 57, 196)
id pixel	4	5	6	7
Pixel	(106, 214, 52)	(191, 100, 101)	(47, 154, 149)	(211, 150, 166)

Questions

Reconstruisez le mot de trois lettres à partir des données ci-dessus. Détaillez toute la démarche.

Ex3. Cryptographie - 8 points

Nous avons ici Alice qui discute avec Bob en utilisant un chiffrement asymétrique. Chaque individu a une clé publique et une clé privée.
Alice envoie à Bob le message suivant : $\{\{K\}_{pvAlice}\}_{pkBob}, \{K * M \bmod n\}_{pkBob}$. La clé publique d'Alice et sa clé privée sont respectivement $pkAlice$ et $pvAlice$. La clé publique de Bob et sa clé privée sont respectivement $pkBob$ et $pvBob$. K est un nombre secret généré par Alice. M est un message de deux lettres. La notation $\{x\}_y$ signifie que l'on chiffre le message x avec un algorithme asymétrique paramétré par la clé y.

Questions

1. Supposons que Bob reçoit le message X, Y où $X = \{\{K\}_{pvAlice}\}_{pkBob}$ et $Y = \{K*M \bmod n\}_{pkBob}$.
   (a) Exprimez K en fonction de X, $pkAlice$ et $pvBob$ en utilisant les notations ci-dessus.

(b) Exprimez M en fonction de Y, $pvBob$ et K en utilisant les notations ci-dessus.

2. Application numérique du protocole précédent : Les clés sont des clés RSA. La base utilisée est $n = 113249$. La clé publique d'Alice est $(139, 113249)$. Sa clé privée est $(41299, 113249)$. La clé publique de Bob est $(82639, 113249)$. Sa clé privée est $(79, 113249)$.

   Sachant ceci, Alice a envoyé à Bob le message suivant : 111432, 27038. Détaillez tous vos calculs pour extraire le message de deux lettres. Le procédé pour chiffrer un message est identique à celui vu en première session. Par exemple, pour chiffrer "He" avec une clé publique (e, n), il faut d'abord convertir "He" en octets (exprimés en base 16). Ici, "He" devient 4865 (48 est l'octet de "H" et "65" l'octet de "e"). Ensuite on considère ces deux octets comme un seul bloc de 16 bits et donc comme un entier de 16 bits. Ainsi, "He" devient **18533**. Donc pour chiffrer "He" avec la clé (e, n), il suffira de faire $18533^e \mod n$. Pour reconstruire les caractères à partir de l'entier sur 16 bits, il faut faire exactement l'inverse. Il faut décomposer 18533 en puissances de 16 (sachant qu'il n'y a que 4 blocs de 4 bits). Donc, $18533 = 4 * 16^3 + 8 * 16^2 + 6 * 16^1 + 5 * 16^0$. On retrouve alors les deux octets : **48** et **65**.

Annexe

— Carrés successifs en base 113249 :
  — 111432, 17268, 112456, 62604, 52673, 70927, 5500, 12517, 51922, 1639, 81594, 11873, 86373, 17254, 82144, 34818, 75828
  — 86941, 46225, 81742, 63564, 110772, 20083, 47200, 5672, 8868, 46618, 102863, 55948, 89593, 43027, 41326, 43356, 35834
  — 27038, 31149, 56018, 113032, 47089, 71750, 102707, 36495, 76785, 80036, 58109, 23697, 59267, 46305, 9708, 22096, 16777

— Produits utiles en base 113249 : 5500 * 14244 = **86941** ; 5672 * 88351 = **47** ; 107266 * 112456 = **101310** ; 17268 * 111432 = **107266** ; 21686 * 56824 = **22895** ; 27038 * 31149 = **87098** ; 46225 * 86941 = **93711** ; 56018 * 87098 = **62346** ; 60798 * 102707 = **56824** ; 62346 * 113032 = **60798** ; 62604 * 101310 = **14244** ; 63564 * 93711 = **88351**

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		

FIGURE 1 – ASCII