WEB 2018 (M1 MIASHS)

TD 1 : Codage et cryptographie

Exercise 1. Nous avons intercepté un signal venant d'une planète distante Gliese 667 Cc. Le département de défense a conclu que c'est un message en ASCII (7-bits) codé avec le code de Hamming (7,4). Décoder le message. Est-ce que vous avez toutes les informations nécessaires pour le décoder sans ambiguïté ?

0	0	1	1	1	0	1		1	1	1	0	0	0	0		1	0	0	0	1	0	1		1	0	1	1	1	1	1

1	1	0	0	1	1	0		1	1	0	0	1	1	0		1	1	1	0	0	0	1								

Le tableau ASCII vous est donnée :

USASCII code chart

b_7 b_6 b_5 →	0 0 0	0 0 1	0 1 0	0 1 1	1 0 0	1 0 1	1 1 0	1 1 1
Bits b_4 ↓	b_3 ↓	b_2 ↓	b_1 ↓	Column → / Row ↓	0	1	2	3	4	5	6	7
0	0	0	0	0	NUL	DLE	SP	0	@	P	`	p
0	0	0	1	1	SOH	DC1	!	1	A	Q	a	q
0	0	1	0	2	STX	DC2	"	2	B	R	b	r
0	0	1	1	3	ETX	DC3	#	3	C	S	c	s
0	1	0	0	4	EOT	DC4	$	4	D	T	d	t
0	1	0	1	5	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	6	ACK	SYN	&	6	F	V	f	v
0	1	1	1	7	BEL	ETB	'	7	G	W	g	w
1	0	0	0	8	BS	CAN	(	8	H	X	h	x
1	0	0	1	9	HT	EM	)	9	I	Y	i	y
1	0	1	0	10	LF	SUB	*	:	J	Z	j	z
1	0	1	1	11	VT	ESC	+	;	K	[	k	{
1	1	0	0	12	FF	FS	,	<	L	\	l	|
1	1	0	1	13	CR	GS	-	=	M	]	m	}
1	1	1	0	14	SO	RS	.	>	N	^	n	~
1	1	1	1	15	SI	US	/	?	O	_	o	DEL

Exercise 2. Une collision entre deux particules capricieuses dans l'accélérateur CERN a ouvert un portail a une dimension cachée de l'univers. Plusieurs chercheurs sont traversé le portail mais aucun veut rentrer. Les chercheurs ont alors décidé d'envoyer une sonde pour inspecter la nouvelle dimension. Malheureusement, l'envoie d'un signal électromagnétique est possible uniquement dans une seule direction (de la dimension cachée vers la nôtre) et en plus pour tout message de 8 bits 2 erreurs peuvent être introduites. Proposes un code qui permettra une bonne réception de tout message.

Exercise 3. Est-ce que le code de Hamming (7,4) est capable de détecter 2 erreurs de transmission (par message) ? Si oui, est-il capable de les corriger ?

Exercise 4. Idem pour 3 erreurs.

Exercise 5. Télécharger le fichier `alice.txt` de la page du cours et vérifier l'intégrité du fichier avec le hashage MD5 (le code est dans `alice.txt.md5`).

Exercise 6. Modifier le fichier `alice.txt`, recalculer le code MD5 et comparer avec le code cible. Commencer avec un changement d'un seul caractère et ensuite faire des changement de plus en plus importante. Est-ce qu'il y a une dépendance entre l'ampleur des changements du texte et l'ampleur du changement dans le code MD5 ?

Exercise 7. Refaire l'exercice avec le hashage SHA (1 ou 2) et CRC32.

Exercise 8. Alice a signé le fichier `alice.txt` avec sa clé privée (`lewis_carrol_id`) avec a commande

```
cat alice.txt | openssl dgst -sha512 -hex -sign lewis_carroll_id > alice.sign.txt
```

La signature électronique se trouve dans le fichier `alice.txt.sign`. La clé publique de Lewis Carrol se trouve dans le fichier `lewis_carroll_id.pub`. Vérifier que l'authenticité du fichier. Ensuite composer un message à Lewis Carrol en lui remerciant pour son oeuvre et chiffrer le message avec sa clé (publique).

Exercise 9. Créer votre propre (paire de) clé RSA avec la commande `ssh-keygen` et ensuite utiliser la clé publique d'un de vos camarades pour lui envoyer un message secret. Déchiffrer sa réponse.

Exercise 10. Idem mais en plus avec les signatures.

Exercise 11. Proposer un protocole sécurisé pour achats avec une carte bancaire sans et avec une pouce.