Exercice 1/ Chiffrement par d´ecalage (C´esar)

1/ QF WJTSYWJW JXY UWJAZJ F QF HFKJYJNFW

2/

K= 15
RGNEIDVGPEWXTRAPHHXFJT
CRYPTOGRAPHIECLASSIQUE

3/ k= 10
SVOXFYIKNKXCVKVSQEBSOKMRODOBNOCCYVNKDC
IL ENVOYA DANS LA LIGURIE ACHETER DES SOLDATS

Exercice 2: . Chiffrement par substitution

1. “la rencontre est prevue a la cafeteria"
   BX CHSYFSMCH HVM X BX YXPHMYCZX

   2)Non , il est impossible de déchiffrer le message YHVMQUVMH sans connaitre la clé.

YHVMQUVMH --> C'est juste

Exercice 3: Chiffrement de Vigenère

1. clé : POULE

	Lettre en clair																								
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Lettre de la clé	Lettres chiffrées (au croisement de la colonne *Lettre en clair* et de la ligne *Lettre de la clé*)																								
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

LA RENCONTRE EST PREVUE A LA CAFETERIA
PO LE POULEPO ULE POULEP O UL EPOULEPO

--> AOLPRRCHEVTSKETGSPFIPZUNEUTNPVXO

2. a)Non , il est impossible de déchiffrer le message "BAUNBEKLZLQSKQKEBGCJYHVSKR" sans connaitre la clé.

b) clé " TNCY"
BAUNBEKLZLQSKQKEBGCJYHVSKR

-->INSPIRINGYOURDIGITALFUTUR

Exercice 4 : Message confidentiel et authentifié

a) Le problème est que bob n'a aucune certitude qu'il échange bien avec Alice, car il se peut qu'entre leur message ils ont subit une attaque MIM(man in the middle) qui interceptent et déchiffre leur messages sans qu'ils s'en rendent compte car il les rechiffre avec leur propres clés publiques et le leur transmet normalement.

Exercice 5 :SSH

1. --> Le client fait une requête de connexion au serveur
   --> Le serveur envoie un défi : un message ou une question au client, appelée un "défi", pour vérifier son identité.

-->Le client signe le défi avec sa clé privée : Le client prend ce défi et le signe avec sa clé privée

-->: Le client envoie cette signature au serveur.

-- >Le serveur vérifie la signature : Le serveur utilise la clé publique du client (qu'il connaît déjà) pour vérifier si la signature reçue correspond bien au défi qu'il a envoyé. Cela prouve que le client possède la clé privée associée à cette clé publique.

-->La réponse : soit la signature est correcte et il réussit à se connecter avec le compte SMITH , soit elle est incorrecte et le message d'erreur "authentification a échoué " apparait

2.

Avant qu'une connexion SSH soit établie, le client et le serveur doivent échanger des clés publiques pour vérifier l'identité du serveur, négocier des algorithmes de chiffrement pour sécuriser la communication, puis procéder à l'authentification du client via mot de passe ou clés publiques/privées. Une fois ces étapes réussies, la connexion SSH est pleinement établie et sécurisée

3. -->Authentification par mot de passe

le client peut envoyer son mot de passe au serveur. Le serveur, après avoir reçu le mot de passe, le comparerait avec le mot de passe stocké pour l'utilisateur **SMITH**.
Avantages : Simple à mettre en place, facile à comprendre.

- Inconvénients:
  -Moins sécurisé que l'authentification par clé publique.
- Le mot de passe peut être intercepté si la communication n'est pas sécurisée, même si SSH chiffre généralement la communication.
- L'utilisateur doit mémoriser son mot de passe, ce qui peut être contraignant.

**Exercice 6 :

On estime qu'il y a environ 10 000 prénoms fréquents (en fonction de la base de données utilisée).
Chaque essai dure une seconde.
Total du temps 10 000/60/60 = 2,78 heures.
le déchiffrement du mot de passe nécessitera a peu prés 2,8 heures.

Ici, on suppose qu'un dictionnaire renferme environ 100 000 mots fréquemment utilisés. Total du temps 100 000/60/60 = 27,78 heures. Ainsi, le déchiffrement du mdp nécessitera approximativement 28 heures. Un mot de passe avec 4 chiffres peut contenir 10^4=10 000 combinaisons possibles. Le résultat est identique à celui des prénoms.

Un mot de passe alphanumérique, comprenant 26 lettres majuscules, 26 lettres minuscules et 10 chiffres, ainsi que 15 signes de ponctuation, offre un total potentiel de 77 caractères. Pour un mot de passe composé de 8 caractères, le total