1 Chiffrer et déchiffrer

a) Pour chiffrer un message composé de lettres majuscules de A à Z, on utilise le système de substitution suivant. A chaque lettre de l'alphabet, on fait correspondre une autre lettre, par exemple:

A→K, B →H, C →D, D→F, E →A, F →P, etc.

On suppose ici que chaque lettre est utilisée une et une seule fois, i.e., qu'il y a une correspondance univoque entre l'alphabet d'origine et celui utilisé pour le chiffrement.

Une attaque par force brute de ce système permet de déchiffrer un message en une heure en testant toutes les substitutions possibles. Combien d'heures cette même attaque nécessitera-t-elle pour déchiffrer un message écrit avec un alphabet de 28 lettres et chiffré avec la même méthode ?

b) Supposons qu'une clé K d'une longueur de 20 bits soit utilisée pour chiffrer un message binaire d'une longueur sensiblement plus grande (on ne spécifie pas ici le système de chiffrement utilisé). Supposons également qu'avec une attaque par force brute avec un ordinateur donné, il soit possible de trouver la clé K (et donc de déchiffrer le message) en 5 minutes. Si maintenant une clé K′ deux fois plus longue est utilisée pour chiffrer le message, combien de temps sera nécessaire pour déchiffrer le message avec une même attaque par force brute, si on dispose d'un ordinateur cent fois plus puissant que le premier (i.e., un ordinateur effectuant cent fois plus d'opérations par seconde) ?

2 Protocole d'échange de clé de Diffie-Hellman avec 3 personnes

Au cours, nous avons vu comment 2 personnes peuvent parvenir à se mettre d'accord sur une clé secrète K en communiquant uniquement sur un canal public, si l'on fait l'hypothèse que l'exponentiation modulo P (avec P un grand nombre premier) est une opération à sens unique, ce qui veut dire la chose suivante :

« Même en connaissant les valeurs de P et N_1, N_3 (compris entre 1 et P−1) satisfaisant la relation $N_1^{N_2} (mod\ P) = N_3$, il est très difficile de retrouver la valeur de N_2. »

Dans cet exercice, on vous propose de réfléchir à un protocole similaire permettant à 3 personnes de se mettre d'accord sur une clé secrète commune K, tout en ne communiquant que sur un canal public.

3 Routage

a) On considère un réseau comprenant 6 nœuds nommés A, B, C, D, E et F. On connaît (en partie) leurs tables
de routage:

A		
dest	dir	dist
C	B	2
E	F	2
D	B	3

B		
dest	dir	dist
D	C	2
F	A	2
E	C	2

C		
dest	dir	dist
F	E	2
A	B	2

et

D		
dest	dir	dist
B	C	2
E	C	2
F	C	3
A	C	3

E		
dest	dir	dist
D	C	2
A	F	2
B	C	2

F		
dest	dir	dist
B	A	2
C	E	2
D	E	3

Le nœud B tombe en panne et n'est plus utilisable. Tous les autres nœuds sont avertis de cette panne et leurs tables de routage sont mises à jour de façon à éviter le nœud B.
Existe-t-il encore une route de A à D après la panne, et si oui, quelle est sa longueur?

b) On considère maintenant un autre réseau dans lequel se trouvent plusieurs nœuds A, B, C, ..., N, O. On connaît en partie les tables de routage des noeuds A, F et H, qui sont:

A		
dest	dir	dist
B	C	2
D	C	5
N	x	y

F		
dest	dir	dist
J	O	2
L	K	2
M	N	2

H		
dest	dir	dist
D	I	2
C	B	2
F	J	3

En se basant uniquement sur un strict minimum de liens entre nœuds qui doivent exister selon les tables ci-dessus (i.e., sans imaginer d'autres liens non-justifiées par ces tables), pouvez-vous déduire les valeurs de x et y dans la table de routage de A?

Indication (à lire que si vous ne voyez pas comment faire!): Dans cet exercice, pour construire le réseau à partir des tables de routage, vous devez d'abord vous focaliser uniquement sur les indications des noeuds qui sont à distance 2 dans les tables (puis vérifier avec les autres que le réseau que vous avez construit est cohérent).