Université Paris DESCARTES - UFR de mathématiques et Informatique

Licence 3 – Spécialité Informatique

Réseaux Avancés – durée 01h30

Examen partiel du 15/03/2018- Sans documents

Exercice 1 (1.5 points)

Le message suivant a été chiffré avec l'algorithme de César. Expliquer la démarche à suivre et donner le texte en clair, sachant que vous ne connaissez pas **la clé** de chiffrement.

UGFFSAKKWRNGMKDSTGFFWNAWADDWDGYAIMWVWBMDAWF

Exercice 2 (2 points)

Le texte suivant a été chiffré avec l'algorithme de Vigenère et une clé de longueur 2 (2 caractères). Sachant que le texte en clair est écrit en Français, trouver le texte lisible et donner la clé. Expliquer clairement la démarche suivie pour trouver la clé et **pour déchiffrer**.

HUZPVUKBZEEMVDZRVCVQLIVSKAIRZVV

Exercice 3 (3 points)

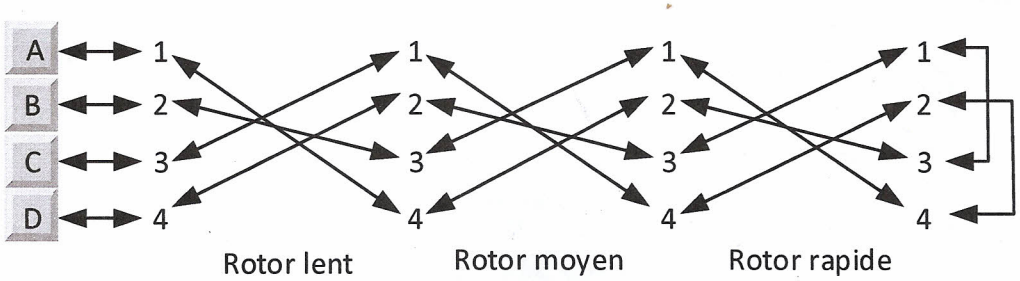
L'algorithme de "PlayFair" est utilisé pour transformer un message lisible en un cryptogramme qui résiste à l'analyse fréquentielle via une technique polyalphabétique. Déchiffrer **le message** suivant et donner le texte en clair, sachant que la lettre "parasite" ("W") partage la case de la lettre "X".

CSYVGVYKNLSLCQLSHBQCDTCDPEULHUULYPVUQTLRLNBELCQPGV FBSXFCGODU

La clé est cachée dans le sujet. Saurez-vous la retrouver pour déchiffrer le message? Comment s'appelle cette technique de communication ?

Exercice 4 (3 points)

"Enigma" **est le** nom de la machine de cryptographie utilisée durant la seconde guerre mondiale par l'Allemagne nazie et ses alliés.



Donner le résultat du chiffrement de la séquence "AABAAA" par le modèle simplifié donné par le schéma précédent.

Exercice 5 (1.5 points)

Le message suivant a été chiffré avec l'algorithme de transposition en zig-zag de niveau 4. Donner le **nom de l'algorithme** de chiffrement et déchiffrer le cryptogramme suivant :

ENNOE LARTR TEDOR CMNND ASRER RIARE ETRTI EMOTN MRRTE ARNIR NEREE EEPEE

Université Paris DESCARTES - UFR de mathématiques et Informatique

Licence 3 – Spécialité Informatique

Réseaux Avancés – durée 01h30

Examen partiel du 15/03/2018- Sans documents

Exercice 6 (3 points)

6.1) Indiquer les services de sécurité fournis par le schéma suivant ? Sachant que "K" est **utilisé** comme une clé de chiffrement partagée entre Alice et Bob, E (resp. D) est la fonction de chiffrement (resp. déchiffrement), H est la fonction d'hachage, M représente le texte en clair et MC représente un texte chiffré. Justifier vos réponses et donner l'expression représentant le message qui circule dans le réseau.

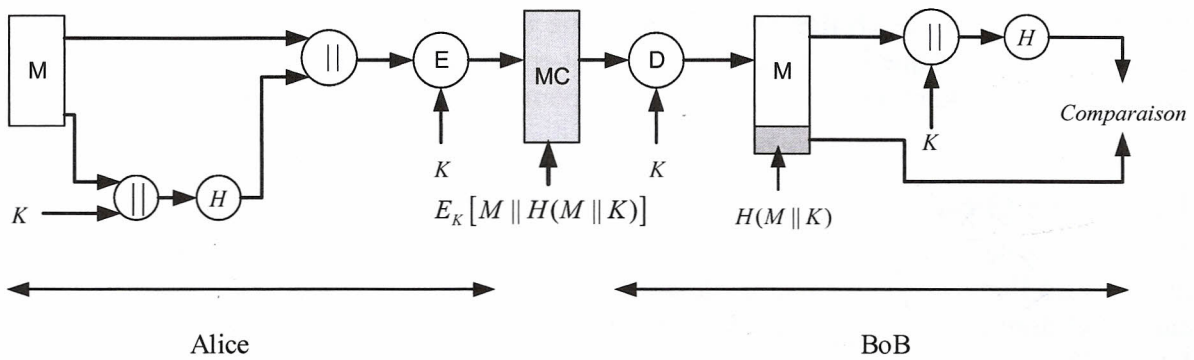


Figure 6.A

6.2) Que représente l'acronyme CIA en sécurité informatique ?

6.3) Classer ces attaques en deux catégories : active et passive

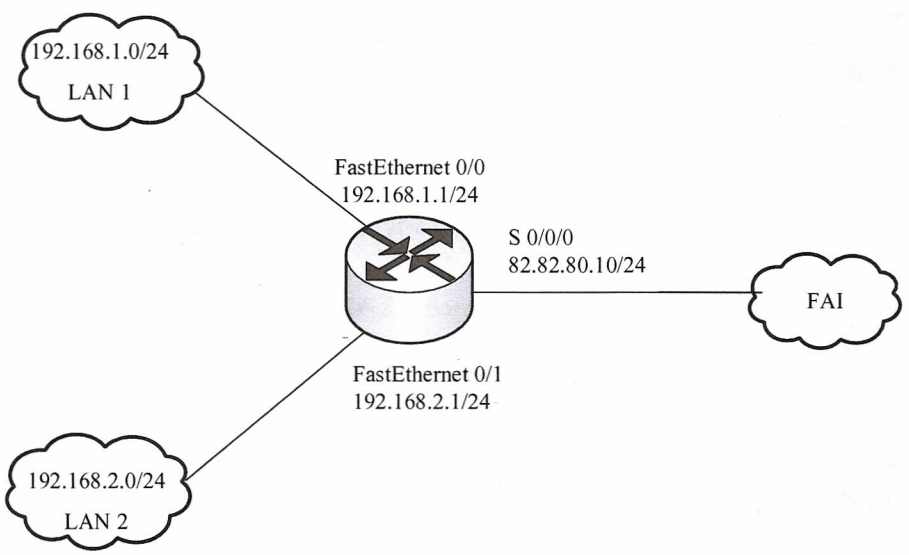
a) Rejeu
b) collecte d'information sur Facebook et twitter
c) Déni de service
d) interception de message

6.4) Le cryptogramme suivant a été chiffré avec l'algorithme "autochiffrement" et la clé "teamo". Déchiffrer le message et donner le texte en clair (écrit en anglais).

BAIEV AKUWI GRKAP IOBPS FWPXA SLFMP TETVL

Exercice 7 (6 points)

On considère le routeur suivant :



7.1 Câblage :

a) Donner le type de câble (droit, croisé ou console) à utiliser pour interconnecter :

a. Un ordinateur à un switch
b. Un switch à un routeur
c. Un routeur à un FAI

b) Peut-on interconnecter deux routeurs **par** un câble Ethernet ? justifier votre réponse

7.2 Configuration du routeur

a) Donner **les** commandes pour modifier le nom du routeur à **Spartiates**
b) Donner la commande pour désactiver la recherche DNS
c) Donner la commande pour sécuriser l'accès au mode privilégié via un mot de passe "cisco"
d) Configurer une bannière du message du jour : "AUTHORIZED ACCESS ONLY"
e) Donner la commande pour sécuriser l'accès local
f) Donner la suite des commandes pour sécuriser et activer l'accès distant
g) Configurer les interfaces FastEthernet 0/0, FastEthernet 0/1 et Serial 0/0 avec les adresses IP indiquées sur le schéma. N'oublier pas de configurer l'horloge si besoin est.

7.3 Fichiers de configuration

a) Un routeur comprend deux fichiers de configuration. Donner le nom de chaque fichier ainsi que l'emplacement de ce fichier (type de mémoire) ?
b) Lequel de ces 2 fichiers de configuration est utilisé au démarrage ? lequel contient les modifications que vous venez d'effectuer ?
c) Dans quelle mémoire se trouve le système d'exploitation Cisco IOS ?

7.4 Dans la suite de cet exercice, on suppose que toutes les interfaces des routeurs et des ordinateurs ont été configurées correctement avec les adresses IP indiquées dans le schéma. Aucun protocole de routage n'a été configuré par l'administrateur pour l'instant.

a) Est-ce qu'un ordinateur dans le LAN 1 pourra "pinger" un ordinateur dans le LAN 2 ? Justifier votre réponse.
b) Est-ce qu'un ordinateur dans le LAN 1 pourra "pinger" un le serveur DNS de google (@IP=8.8.8.8) ? Justifier votre réponse.