Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

Exercice 1 : Chiffrement

1. Que représente l'acronyme CIA en sécurité *informatique* ?
   C : Confidentialité
   I : Integrité
   A: Disponibilité

2. Classe ces attaques en deux catégorie**s** : active et passive
   a. Rejeu : active
   b. Collecte d'information sur Facebook et twitter : pasive
   c. Déni de service : active
   d. Interception de message : passive

3. 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
   teamo

   I WISH SOMEBODY WOULD TELL ME WHAT IT MEANS
   Teamo: je t'aime

Exercice 2 : Chiffrement

Le message suivant a été **c**hiffré 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

ET ENTENDRE TON RIRE COMME ON ENTEND LA MER S' ARRETER REPARTIR EN ARRIERE

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

Exercice 3 : Stéganographie

La stéganographie est la science qui s'intéresse à la manière de cacher une information à l'intérieur d'une autre information, afin que sa transmission n'éveille pas les soupçons.
George Sand, Maîtrisant parfaitement l'écriture, écrivait des poèmes à Alfred de Musset :

Cher ami,
Je suis toute émue de vous dire que j'ai
bien compris l'autre jour que vous aviez
toujours une envie folle de me faire
danser. Je garde le souvenir de votre
baiser et je voudrais bien que ce soit
une preuve que je puisse être aimée
par vous. Je suis prête à montrer mon
affection toute désintéressée et sans cal-
cul, et si vous voulez me voir ainsi
vous dévoiler, sans artifice, mon âme
toute nue, daignez me faire visite,
nous causerons et en amis franchement
je vous prouverai que je suis la femme
sincère, capable de vous offrir l'affection
la plus profonde, comme la plus étroite
amitié, en un mot : la meilleure épouse
dont vous puissiez rêver. Puisque votre>
âme est libre, pensez que l'abandon ou je
vis est bien long, bien dur et souvent bien>
insupportable. Mon chagrin est trop
gros. Accourrez bien vite et venez me le
faire oublier. À vous je veux me sou-
mettre entièrement.
Votre poupée

Trouver le message caché dans ce texte.

Exercice 4 : Service de sécurité

Alice (resp. Bob) utilisent un système de chiffrement symétrique avec K_{AB} comme secret partagé. Quels sont les services de sécurité correctement fournis par les opérations suivantes, dans lesquelles E signifie ″algorithme de chiffrement″ et H ″fonction de hachage″ :

a) $E_{k_{AB}}[M]$

Un secret partagé entre deux personnes n'est plus secret

C : Confidentialité => chiffrement : oui, la confidentialité est fournie via le chiffrement du message (**E** : **E**ncrypt). Encrypter (chiffrer)

~~I : Intégrité : non, le MitM est capable de supprimer un paragraphe sans avoir le besoin de comprendre le contenu de ce paragraph et le récepteur sera incapable de détecter cette suppression~~

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

A : Authentification : Oui, la preuve d'identité est l'utilisation de la clé de chiffrement K_{AB}
~~N: Nonrepudiation n'existe pas~~

b) $M \,||\, H(M)$

(I love you bob || ee331a8824c18a5e57402f91d2a2cc07) = > Trudy => =>BOB
~~I: Non parcequ'on peut modifier le message et le digest M'||E[M']~~
~~A: non il n'y a pas une utilisation d'une preuve d'identité~~
~~C: confidentialité: non pas de confidentialité parce que le message n'est pas chiffré (le message est lisible).~~
~~Non repudiation~~

c) $E_{k_{AB}}\left[M \,||\, H(M)\right]$ =

E(I love you bob || ee331a8824c18a5e57402f91d2a2cc07) == > MitM = > D(Recu)= M' || H(M)

H(M')= EM'
H(M)=EM

Integrité : Oui, l'empreinte est chiffrée et l'attaquant ne peut pas générer une autre empreinte valide et la chiffrer
Confidentialité : oui le message est chiffré
Authentification : oui via l'utilisation d'une clé comme une preuve d'identité
~~Non-repudiation~~

d) $M \,||\, E_{AB}\left[H(M)\right]$

Confidentialité : non le message circule en claire
Intégrité : Oui il y a un mécanisme de contrôle d'intégrité, parcequ'il ne possède pas la clé
Authentification : oui via l'utilisation d'une clé de chiffrement comme preuve d'identité
~~Non-repudiation~~

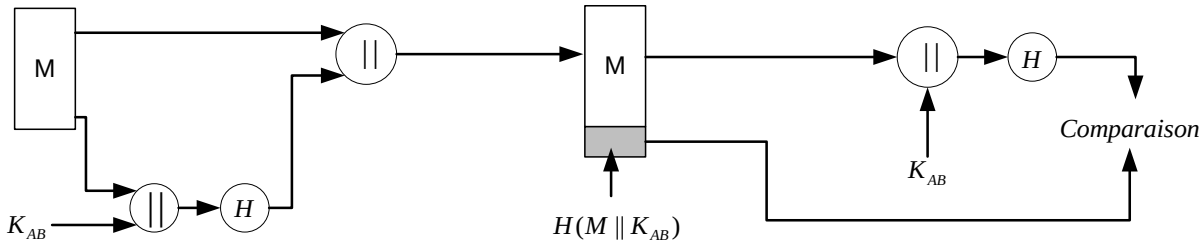
e) M || H(M||k_{AB})

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

Confidentialité : déjà il n'y a pas de confidentialité (demander à jordan), le message est en claire
Intégrité : Oui, le Mitm est incapable de générer une empreinte valide parce qu'il ne possède pas la clé
~~Nonrepuidation~~
Authentification : Oui, via l'utilisation d'une clé comme preuve d'identité
M' || H(M'||K_{AB}) la clé est inconnue par le Mitm



Exercice 5 : Authentification

Alice et *Bob* sont deux correspondants se partageant un secret *K*. Ils utilisent le mécanisme suivant : *Alice* envoie son identité accompagnée d'un nombre aléatoire N_A à *Bob*, qui renvoie en retour son identité, un nombre aléatoire N_B et le nombre envoyé par *Alice* chiffré avec la clé partagée *K*. *Alice* renvoie enfin à *Bob* le nombre N_B chiffré avec la clé partagée *K*.

a) *A* et *B* sont-ils mutuellement certains de leurs identités respectives ?

b) Soit un attaquant *C* placé entre *Alice* et *Bob*, interceptant le trafic et se faisant passer pour *Alice* auprès de *Bob* et pour *Bob* auprès de *Alice*. *C* peut-il pénétrer les communications entre *Alice* et *Bob* dans le cas de l'échange du a) ?

Exercice 6 : cryptanalyse

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

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.

HU=QU
ZP=IP
VU=EU
KB=TB
ZE=IE
EM=NM
VD=ED
ZR=IR
VC=EC
VQ=EQ
LI=UI
VS=ES
KA=TA
IR=RR
ZV=IV
V=E

QUI PEUT BIEN ME DIRE CE QUI EST ARRIVE
Lettre 1 : decalage de 17
Lettre 2 : decalage de 0
RA : Réseaux Avancés

6V et 4z
E=> V
ABCDE FGHIJKLMNOPQRSTUVWXYZ
R

QIETI NEIEE UETRI E

Exercice 7 : cryptanalyse

Vous avez intercepté le message suivant :

RRMWU
SZYHT

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

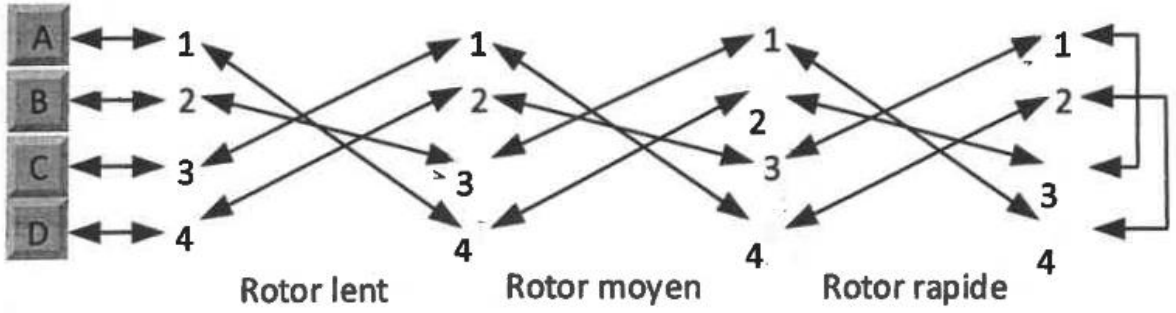
```
GVMHK
TGYIJ
KZYJX
KANAO
HEYHK
ZRAPA
DRHSX
UVNHR
KFXXY
ZVHRZ
OBHHY
UPCPR
KFHTV
KHPTT
ZRNGK
LBHSK
KFKJK
YHLAA
ZVFXZ
KPIBS
AAY
```

```
LES HOMMES NAISSENT ET DEMEURENT LIB RES ET EGAUX EN DROITS
   LES DISTINCTIONS SOCIALES NE PEUVENT ETRE F ONDEES QUE
   SUR L UTILITE COMMUNE
```

Sachant que le texte en clair est écrit en français, et l'algorithme de chiffrement est Vigenère, et que la longueur de la clé est 5. Déchiffrer ce message en expliquant la démarche. (Le résultat du déchiffrement sans la démarche sera considéré faux)
Le classement des lettres selon leur fréquence d'apparition en français : E S A I T N R U L O D C P M V Q F B G H J X Y Z W K. Le tableau Vigenère est donné en annexe pour vous aider.

Exercice 8 : Enigma

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



Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

Donner le résultat du chiffrement de la séquence AABAAA par le modèle simplifié donné par le schéma précédent.
@UBUTNU
@IP (@logique de taille 32 bits ou 4 bytes (bytes = 8bit) =4octets)= 192.168.1.105
@MAC @physique @ethernet : ether 08:00:27:aa:3c:d5 de taille 6 octets : 48bits

ping 192.168.1.105
arp -n
Telnet (23), FTP(21), SSH(22), http(80), HTTPS (443), DNS (53), SMTP (25), IMAP (143), SNMP 161

netstat -antp (chercher :23)
numero de port utilisé par telnetd :23
protocole de transport : tcp (recommandé avec accusé de reception)

tout est lisibile : login et mot de passe et resultat des commandes
selectionner un paquet telnet => clique droiten => suivre > flux TCP

exo3 :
nestat -antp (21)
service vsftpd status
tcp

4. Oui, oui,
   Le login et le mot de passe, nous avons ajouter un filtre d'affichage :ftp et ca sauter à l'œil
   Sinon, pour les aveugles ftp contains pass et sinon, on sélectionne une ligne de wireshark ftp et on fait une clique droite, suivre, flux tcp => on voit les logins, mdp et commandes mais pas le contenu du fichier, parce que c'est dans un autre Protocole qui s'appele FTP-data
   ftp-data est utilisé pour le transfert des fichiers (il utilise le port numéro 20)

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2

Université Paris Descartes – UFR de mathématiques et Informatique

L3 – Sécurité et Réseaux

TD/TP n°2