**Université Paris Descartes – UFR de mathématiques et Informatique**

**L3 – Réseaux avancés**

**TD/TP n°2**

## Exercice 1 : Chiffrement de Vigenère

Vous avez intercepté ce message chiffré avec l'algorithme de Vigenère. Déchiffrer le message sachant que la clé est ″RPS″ :

*CXFKTFKXGEKSLIDVUSZI*

## Exercice 2 : Auto-chiffrement

Déchiffrer le message texte suivant, sachant qu'il est chiffré avec l'algorithme d'auto chiffrement et que la clé utilisée est ″RPS″.

*CPUCYRKYCTLLSPCKXPSKEDVWHGUCRKCGNRDYFEEYW*

## Exercice 3 : Auto-chiffrement

Déchiffrer le message suivant, sachant qu'il est chiffré avec l'algorithme d'auto-chiffrement, et qu'il y a eu une indiscrétion (clé de chiffrement: ″DESCARTES″) :

*OEKVEXTRGRRSILOERGZUEUHQVIHTVWJRQEEEEJUYLVZEHWRIYXNZWMFAAXUE*

## Exercice 4 : Chiffrement de PlayFair

Soit un système polyalphabétique qui utilise une matrice 5x5 avec un *mot-clé* suivi des autres lettres de l'alphabet (avec W et X dans la même case). Chaque groupe de 2 lettres est codé par la lettre à l'intersection de la ligne de la première et la colonne de la seconde puis à l'intersection de la ligne de la seconde et de la colonne de la première. Si les deux lettres tombent sur la même ligne, on remplace chacune par celle de droite (avec rotation circulaire) ; Si les deux lettres tombent sur la même colonne, on remplace chacune par celle de dessous (avec rotation circulaire). En cas de lettre double et en cas de lettre unique (nombre total de lettres impair), une lettre ″parasite″ est insérée (W).
Étant donné qu'il y a eu une indiscrétion, vous connaissez la clé : ″Intelligent″.
Déchiffrer le message suivant :

*IL OP IL NI IZ NE QP YO IQ XI IL FS LA TY*

## Exercice 5 : Chiffrement de Rail Fence

Rail Fence est une forme de transposition qui consiste à écrire les lettres en "Zig-Zag". Déchiffrer le message suivant, sachant que la clé est 3 (niveau=3).

*LOSST ERLEE XRSEH MENIS NEDMU ETIRS TGUED OTSMA ETENB EANI*

## Exercice 6 : Chiffrement via transposition de la matrice

L'exemple ci-dessous utilise un système de chiffrement avec transposition de colonnes pour protéger des données confidentielles :

*MGCDECSSFTSENN*EEOELEATII*

Étant donné qu'il y a eu une indiscrétion, vous connaissez la clé 31542.

Déchiffrez le message : pour le chiffrement, on écrit le message en ligne et on le lit en colonnes.

## Exercice 7 : cryptanalyse

Vous avez intercepté le message suivant :

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

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 : 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 calcul, 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 où je …
>
> Votre poupée

Trouver le message caché dans ce texte.

## Exercice 9 : Services de sécurité

Alice (resp. Bob) utilisent également un système symétrique avec $K_{AB}$ comme secret partagé.

**Université Paris Descartes – UFR de mathématiques et Informatique**

**L3 – Réseaux avancés**

**TD/TP n°2**

Quels sont les services des sécurités correctement fournis par les opérations suivantes, dans lesquelles E signifie ″algorithme de chiffrement″ et H ″fonction de hachage″ :

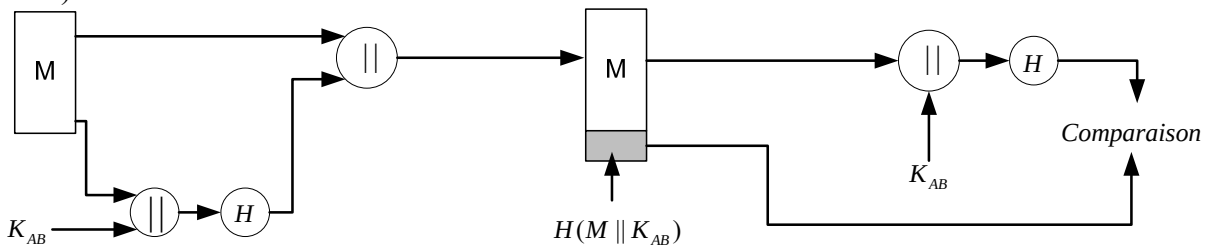
a) $E_{k_{AB}}[M]$

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

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

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

e)




## Exercice 10 : 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 *A* et *B* dans le cas de l'échange du a) ?

## Exercice 11 : Chiffrement Par substituions (à rendre)

Vous êtes maintenant des experts pour casser des systèmes cryptographiques. Voici un exemple avec un simple code de substitution : il contient, en français, le texte le plus célèbre de l'histoire des idées politiques :

```
IGY SWFFGY JCPYYGJX GX AGFGMBGJX IPEBGY GX GRCMK GJ ABWPXY. IGY
APYXPJNXPWJY YWNPCIGY JG LGMOGJX GXBG UWJAGGY ZMG YMB I MXPIPXG
NWFFMJG. IG EMX AG XWMXG CYYWNPCXPWJ LWIPXPZMG GYX IC
NWJYGBOCXPWJ AGY ABWPXY JCXMBGIY GX PFLBGYNBPLXPEIGY AG I SWFFG.
NGY ABWPXY YWJX IC IPEGBXG, IC LBWLBPGXG, IC YMBGXG, GX IC
BGYPYXCJNG C IWLLBGYYPWJ. IG LBPJNPLG AG XWMXG YWMOGBCPJGXG
BGYPAG GYYGJXPGIIGFGJX ACJY IC JCXPWJ. JMI NWBLY, JMI PJAPOPAM
JG LGMX GKGBNGB A CMXWBPXG ZMP J GJ GFCJG GKLBGYYGFGJX.
```

## Exercice 12 : Chiffrement Par substituions (à rendre)

Voici un nouvel exemple, toujours écrit en français, et avec un simple code de substitution :

**Université Paris Descartes – UFR de mathématiques et Informatique**

**L3 – Réseaux avancés**

**TD/TP n°2**

SMUJM GJHL M SPPCGSCU DSW S OJPNCP. CL SLLKNS. WJM YSQ NSPZKSCU NCMKCU GCMFU. CL DJKWWS KM DPJRJMO WJKDCP, W SWWCU OSMW WJM LCU, W SDDKHSMU WKP WJM DJLJVEJM. CL DPCU KM PJNSM, CL L JKGPCU, CL LKU; NSCW CL M H WSCWCWWSCU ZK KM CNAPJFLCJ VJMRKW, CL AKUSCU À UJKU CMWUSMU WKP KM NJU OJMU CL CFMJPSCU LS WCFMCRCVSUCJM.
CL SASMOJMMS WJM PJNSM WKP WJM LCU. CL SLLS S WJM LSGSAJ; CL NJKCLLS KM FSMU ZK'CL DSWWS WKP WJM RPJMU, WKP WJM VJK.
WJM DJKLW ASUUSCU UPJD RJPU. CL SGSCU VESKO. CL JKGPCU WJM GSWCWUSW, WVPKUS LS MKCU. CL RSCWSCU OJKB. KM APKCU CMOCWUCMVU NJMUSCU OK RSKAJKPF. KM VSPCLLJM, DLKW LJKPO ZK KM FLSW, DLKW WJKPO ZK'KM UJVWCM, DLKW DPJRJMO ZK KM AJKPOJM, MJM LJCM, WJMMS UPJCW VJKDW. OK VSMSL WSCMU-NSPUCM, KM VLSDJUCW DLSCMUCR WCFMSLSCU KM VESLSMO ZKC DSWWSCU.
WKP L SASUUSMU OK GSWCWUSW, KM SMCNSL SK UEJPSB CMOCFJ, S L SCFKCLLJM WSRPSM, MC KM VSRSPO, MC KM VESPSMÇJM, NSCW DLKUJU KM SPUCWJM, W SGSMVSCU, UPSCMSMU KM APCM O SLRS. CL W SDDPJVES, GJKLSMU L SDLSUCP O KM VJKD GCR, NSCW L SMCNSL DPCU WJM GJL, OCWDSPSCWWSMU OSMW LS MKCU SGSMU ZK CL SCU DK L SWWSCLLCP.

De même que dans l'exercice précédent, la ponctuation et les espaces ont été laissées pour vous faciliter la tâche… A vous de déchiffrer.

**Université Paris Descartes – UFR de mathématiques et Informatique**

**L3 – Réseaux avancés**

**TD/TP n°2**

# Annexe :

| 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 |

*Tableau I : Table de Vigenère*