Exercices : thème 3 - Question 7

Question 7 : En quoi les systèmes d'information transforment-ils les échanges entre les acteurs de l'organisation ?

Au travers de ces exercices, nous allons de fait combiner et traiter deux questions du programme, la question 7 d'une part et la question 2, à savoir « Les évolutions technologiques sont-elles exemptes de risques pour l'organisation » ?
Au sein des organisations, le remplissage de document papier ne cesse de décroître au profit de la saisie informatique. Au partage de documents papier succède pas-à-pas le partage de documents en ligne. Aux échanges verbaux viennent s'adjoindre les échanges par messageries instantanées. Etc. Aussi, tâchons de nous faire une idée des changements que les technologies ont opérés et continuent d'opérer sur les échanges entre individus, en particulier au sein d'une organisation.

Exercice 1 : nouveaux outils et nouveaux modes de travail

Sujet : Madame HIGHTECH, gérante de la société ZAHIA DIAMOND, PME en pleine croissante, constate que la communication au sein de la société n'est pas assez performante et que ses équipes peinent à communiquer efficacement. De fait, le SI de la société demeure relativement rudimentaire. Les employés ont accès à des postes informatiques interconnectés en réseau mais peu de services leur sont offerts.

Questions :

1. Partage de documents

Lorsqu'un chargé d'affaires part en mission, il a besoin d'emmener avec lui différents documents techniques ou réglementaires. Ces documents sont disponibles en format numérique. Des tablettes sont à la disposition des chargés d'affaires. Celles-ci leur permettent en outre de présenter ces documents.

Malheureusement, lorsqu'un chargé d'affaires a besoin de documents, il est obligé de les transférer sur la tablette. Il doit encore récupérer ces documents sur son poste informatique ou les demander à son responsable.

1.1. Citer des exemples de logiciels permettant le partage de documents en ligne.
DropBox, iCloud, Mega, OneDrive, Google Documents

1.2. En quoi l'utilisation de l'une de ces solutions logicielles pourrait s'avérer très utile à l'organisation ?
La mise en place d'une telle solution permet un gain de temps, d'efficacité et d'accessible. En effet, de telles solutions permettent le partage de documents auxquels on peut accéder au moyen d'une simple connexion internet. En l'occurrence, des documents pourront par exemple être mis à la disposition de tous les chargés d'affaires sans pour autant qu'ils n'aient besoin de les réclamer et/ou de les transférer sur leur tablette.

Pour des raisons de confidentialité, Madame HIGHTECH craint de mettre en place une solution telles que celles évoquées dans les deux questions précédentes. En guise d'alternative, elle s'est intéressée à la notion de serveur de fichiers FTP.

1.3. Rappeler le rôle d'un serveur de fichiers et celui du protocole FTP.

Un serveur de fichiers permet de stocker et partager des données et, en particulier, des documents. Le protocole FTP définit quant à lui la façon dont les données doivent être transférées d'un poste informatique vers un serveur de fichiers. En d'autres termes, le protocole FTP définit la façon dont un poste informatique et un serveur de fichiers doivent communiquer pour s'échanger des fichiers.

Rappel de réseau : on parle de serveur FTP (logiciel et matériel permettant le stockage des fichiers) et de client FTP (logiciel permettant de communiquer avec un serveur FTP. Exemple : Filezilla).

1.4. Quelles problématiques, en particulier de sécurité et d'accessibilité, peut poser cette solution ?

En matière d'accessibilité, le problème réside dans le fait que le serveur devra être accessible depuis l'extérieur pour satisfaire aux besoins des chargés d'affaires. En effet, ces derniers ont besoin de pouvoir accéder à des documents lorsqu'ils partent « en mission ».

Le fait que des fichiers, parfois « confidentiels », soient accédés depuis l'extérieur du réseau local de ZAHIA DIAMOND constitue risque de sécurité, à savoir un point d'entrée pour les pirates.

Plus encore, le protocole FTP n'est pas sécurisé, c'est-à-dire que les communications ne sont pas cryptées. Il vaudra mieux utiliser et imposer l'utilisation du protocole SFTP, variante sécurisée du protocole FTP.

Finalement, Madame HIGHTECH, soucieuse de mettre en place une solution informatique évolutive, a décidé de mettre en place un intranet. Une partie de l'intranet sera accessible en extranet. En particulier, des documents, parfois confidentiels, seront mis à la disposition des employés sur l'extranet.

1.5. Rappeler ce que sont respectivement un intranet et un extranet.

Intranet *(« intra » pour interne et « net » pour internet)* : c'est un ensemble de ressources web disponibles sur le réseau local d'une organisation. Il fait intervenir les technologies du web. On qualifie souvent d'intranet un site internet disponible sur le réseau local de l'organisation et accessible uniquement au sein de celle-ci.

Extranet *(« extra » pour externe et « net pour internet)* : c'est un ensemble de ressources web du réseau local d'une organisation mais mises à la disposition d'utilisateurs extérieurs à l'organisation. Un extranet permet aux acteurs internes d'une organisation de mettre à disposition des ressources web au profit d'acteur externes. On parle souvent de sites extranet.

1.6. Expliquer en quoi il est indispensable de rendre l'extranet accessible uniquement en HTTPS.

HTTPS est la version sécurisée du protocole HTTP. En l'occurrence, ZAHIA DIAMOND doit mettre à disposition de ses chargés d'affaires des documents confidentiels. Il importe donc que l'extranet soit convenablement sécurisé, ce qui justifie l'utilisation du protocole HTTPS plutôt que celle du protocole HTTP.

1.7. Qu'est-ce qu'un site internet responsive ? En une phrase, expliquer en quoi le fait que l'extranet évoqué précédemment soit responsive peut s'avérer en l'occurrence très pratique ?

Un site internet responsive est un site qui s'adapte à tous les écrans : ordinateurs, tablettes, mobiles…
Un extranet responsive peut s'avérer très utile aux chargés d'affaires dans la mesure où ils sont amenés à utiliser des tablettes pour consulter les documents.

2. Travail collaboratif

La société ZAHIA DIAMOND est une société industrielle. Sur les lignes de production en particulier, le travail est divisé en tâches élémentaires prises en charge par des ouvriers spécialisés. Chaque ouvrier est ainsi cantonné à la réalisation d'une ou de quelques tâches élémentaires et répétitives. Madame HIGHTECH souhaite rendre ces tâches plus attractives et par là-même améliorer la productivité des ouvriers.

2.1. Quelle(s) distinction(s) faites-vous entre travail coopératif et travail collaboratif ?
Le travail coopératif consiste à diviser les tâches puis à travailler individuellement et de manière très indépendante. La somme des travaux individuels donne le résultat commun.
Le travail collaboratif consiste à définir les tâches en équipe, à négocier et faire le travail ensemble. Il nécessite une implication globale des membres de l'équipe, laquelle définie ses objectifs aussi bien que son travail. Il y a une dynamique de groupe.

2.2. Le mode de travail en production est-il coopératif ou collaboratif ? Justifier.
Il s'agit d'un travail coopératif dans la mesure où le travail est divisé en tâches réalisées par chacun presque indépendamment de l'autre.

Madame HIGHTECH a décidé qu'ouvriers, chef d'atelier et responsable de production, à la fin de chaque semaine, négocieront ensemble les objectifs de production de la semaine suivante. A cette occasion, les ouvriers spécialisés se répartiront les tâches élémentaires de sorte qu'un ouvrier pourra, au fil du temps, être amené à effectuer les différentes tâches de production. Lorsqu'une tâche lui est inconnue, il sera éventuellement accompagné par un ouvrir plus chevronné.

2.3. Ce nouveau mode de travail est-il plutôt coopératif ou collaboratif ? Justifier.
Quoique ce mode de travail demeure relativement coopératif, il revêt un caractère collaboratif. En effet, les ouvriers vont être amenés à s'entraider et ils vont participer à leurs propres objectifs et à leur propre répartition des tâches, ce qui relève du travail collaboratif.

3. Base de connaissances

Madame HIGHTECH a constaté que, ne connaissant pas toujours bien les procédures de l'entreprise, les employés ont tendance à ne pas pleinement les appliquer. En l'état actuel du système d'information, ce dysfonctionnement lui semble inévitable. En effet, les procédures sont en grande partie communiquées de manière orale. Afin de solutionner en partie ce problème, elle souhaiterait intégrer un Wiki à l'intranet de ZAHIA DIAMOND. Les procédures de l'entreprise y seraient décrites au moyen de textes et de schémas. Effectivement, Madame HIGHTECH a découvert qu'il était possible de construire son Wikipedia d'entreprise.

Le *crowdsourcing* est un mot valise construit à partir des termes *wisdom of crowds* (sagesse des foules) et *outsourcing* (externalisation). Il signifie littéralement « externalisation de la production à la foule » et consiste ainsi à confier à des personnes indéterminées une tâche normalement réalisée par l'organisation.

3.1. En quoi Wikipedia est-il une solution basée sur le *crowdsourcing* ?
Wikipedia évolue au rythme des contributions des utilisateurs partout au travers de la planète. Tout le monde peut écrire. Wikipédia externalise sa production au plus grand nombre.

Concernant, la rédaction des contenus du Wiki, Madame HIGHTECH souhaite faire appel à l'intelligence collective. Ainsi, ce sont des employés expérimentés, supposés bien connaître les procédures de l'entreprise, qui participeront à la rédaction des contenus.

3.2. Quelle(s) forme(s) de schémas pourrai(en)t convenir à la représentation des informations à disposer sur ce Wiki ?

On pourrait utiliser des schémas événements-résultats ou des logigrammes.

Exercice 2 : nouveaux outils et nouveaux modes de communication

La société FEDERER est une société industrielle produisant des raquettes de tennis pour le compte de plusieurs marques. Cette société dispose de plusieurs sites (locaux) implantés dans diverses villes d'Europe. Les responsables des différents sites sont souvent amenés à travailler ensemble. Pour ce faire, ces employés n'ont parfois pas d'autre choix que de se réunir.

Afin d'entretenir une dynamique de groupe au sein de la société, la société FEDERER dispose d'un réseau social d'entreprise sur lequel elle diffuse les actualités de l'entreprises et sur lequel elle fait participer ses employés. Pour des raisons pratiques, ce réseau social interne est internationalisé, c'est-à-dire multilingue. Un utilisateur français se verra proposé les contenus en français, un utilisateur allemand les contenus en allemand.

Outre le réseau social interne de la société, les *community managers* (gestionnaires de communauté) de FEDERER animent le site internet et les pages Facebook, Linkedin, Twitter et Google+ de la société. A cet égard, dans le cadre d'interviews, les *community managers* font intervenir des personnes et sociétés reconnues dans le monde du tennis.

Questions :

1. Communication entre acteurs internes

1.1. Qu'est-ce que la visioconférence ?

La visioconférence permet d'avoir une conversation vidéo à plusieurs. Elle intègre souvent des outils complémentaires : présentations partagées, partage d'écran, TBI (tableau blanc interactif)…

1.2. Citer un exemple de logiciel tout public assurant cette fonctionnalité.

Un outil tout public de visioconférence est par exemple Skype.

1.3. Quels seraient les avantages et les inconvénients (ou risques) de la mise en place d'une solution de visioconférence pour une société telle que la société FEDERER ?

L'usage de la visioconférence devrait permettre aux employés des différents sites de la société FEDERER de se réunir sans se déplacer. Cela rend les réunions et les échanges plus faciles. Ils pourraient être tout à la fois plus nombreux et moins onéreux. Toutefois, la visioconférence peut présenter des risques de sécurité si les échanges sont mal sécurisés, en particulier si les sujets abordés sont confidentiels.

2. Communication entre acteurs internes et externes

2.1. Qu'est-ce qu'un *community manager* ? Quel est son rôle ?

Un community manager est un individu qui diffuse l'actualité de l'entreprise sur la toile (réseaux sociaux, blogs, forums, partenaires…) et travaille à véhiculer une image positive de l'entreprise en vue de la promouvoir essentiellement sur internet. Son métier contribue au référencement et à la popularité de l'entreprise.

2.2. En quoi est-il important pour l'organisation d'effectuer ce travail de community management ?
Ce travail est important afin de promouvoir l'entreprise et attirer et/ou fidéliser la clientèle et les partenaires.

2.3. Quel est l'intérêt pour l'organisation de faire intervenir des personnes et société reconnues ?
L'organisation espère profiter de la notoriété de ces personnes. Il s'agit comme d'un transfert de notoriété : « l'ami de mon ami est mon ami ». Ces personnes, ayant une bonne image, la transfert en quelque sorte à l'organisation.

La société FEDERER n'a pas encore modernisé son mode de recrutement. Elle diffuse essentiellement ses offres d'emploi sur le célèbre site de Pôle Emploi ainsi qu'auprès des établissements scolaires professionnels (CFA, lycées professionnels…) et de ceux du supérieur (universités, écoles d'ingénieurs…). Ce mode de recrutement s'avère relativement chronophage.

2.4. Proposer des solutions alternatives.
Il est possible d'envisager de diffuser les offres d'emploi directement sur le site internet de la société FEDERER. Une autre possibilité consiste à rechercher et sélectionner des profils sur les réseaux sociaux professionnels (exemple : LinkedIn) puis rentrer en contact direct avec les personnes ciblées.

2.5. En quoi les solutions proposées à la question précédente constituent des opportunités pour l'organisation ?
Pour l'organisation, un recrutement par les réseaux sociaux permet d'accéder facilement à de multiples profils et ainsi de trouver plus commodément des personnes dont le profil est en adéquation avec un poste à pourvoir. Outre le gain de temps, c'est également un gain qualitatif.

Exercice 3 : nouveaux risques

Contexte :

Comme nous l'avons constaté au travers des exercices 1 et 2, l'évolution des technologies est marquée tout aussi bien par l'avènement de nouvelles opportunités que de nouveaux risques. En particulier, on peut s'interroger quant aux risques en matière de sécurité ou encore de protections des données personnelles et de respect de la vie privée.

On ne veut pour le montrer que les risques de sécurité actuels présentés au travers de l'exemple suivant.

Extrait du Monde :

Une attaque informatique de portée mondiale crée la panique

Des hôpitaux britanniques et des entreprises espagnoles ont été touchés par des virus, vendredi. Ils bloquent l'accès aux fichiers d'un ordinateur afin d'obtenir une rançon.

LE MONDE | 12.05.2017 à 18h43 • Mis à jour le 19.05.2017 à 16h38

Abonnez vous à partir de 1 € Réagir Ajouter Partager (1 208) Tweeter

Les autorités américaines ont mis en garde vendredi 12 mai contre une vague de cyberattaques simultanées qui a touché des dizaines de pays dans le monde, recommandant de ne pas payer de rançon aux pirates informatiques. Ceux-ci ont apparemment exploité une faille dans les systèmes Windows, divulguée dans des documents piratés de l'agence de sécurité américaine NSA.

« Nous avons reçu de multiples rapports d'infection par un logiciel de rançon, a écrit le ministère américain de la sécurité intérieure dans un communiqué. *Particuliers et organisations sont encouragés à ne pas payer la rançon car cela ne garantit pas que l'accès aux données sera restauré. »*

LIRE : Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays

Cette vague d'attaques informatiques de *« portée mondiale »* suscite l'inquiétude des experts en sécurité. Le virus en cause est un *ransomware* (« rançongiciel »), un programme qui bloque l'accès aux fichiers d'un ordinateur en vue d'obtenir une rançon.

« Nous avons relevé plus de 75 000 attaques dans 99 pays », a noté Jakub Kroustek, de la firme de sécurité informatique Avast, sur un blog. Forcepoint Security Labs, autre entreprise de sécurité informatique, évoque de son côté *« une campagne majeure de diffusion d'emails infectés »*, avec quelque 5 millions d'emails envoyés chaque heure répandant le logiciel malveillant appelé WCry, WannaCry, WanaCrypt0r, WannaCrypt ou Wana Decrypt0r.

Questions :

1. Respect de la vie privée

En vue d'assurer la protection des données personnelles, le Législateur y a dès 1978 consacré un texte de loi, la Loi Informatique et Libertés. En vous servant de la page Wikipedia relative à cette loi, répondez aux questions suivantes : https://fr.wikipedia.org/wiki/Loi_informatique_et_libertés.

1.1. Citer les principaux droits reconnus aux utilisateurs par la Loi Informatique et Libertés ? Décrivez chacun d'entre eux.

Droit	Description
Droit d'information	Toute personne a droit de savoir si des informations concernant son identité sont conservées dans un fichier. Toute personne a le droit de savoir de quel fichier il s'agit.
Droit d'opposition	Une personne à le droit de s'opposer, à savoir de refuser, à ce que des informations concernant son identité figurent dans un fichier.

Droit d'accès	Toute personne a droit d'accéder aux informations concernant son identité qui serait stockée au sein d'un fichier.
Droit de rectification	Toute personne a le droit de modifier les informations relatives à son identité dans le fichier qui contient ces informations.

1.2. Quelle institution française est chargée d'assurer le respect de la Loi Informatique et Libertés ?
L'institution chargée de l'application de cette loi est la CNIL (Commission Nationale Informatique et Libertés).

1.3. Quelle(s) type(s) d'information(s) personnelle(s) et sensible(s) un site e-commerce pratiquant le paiement en ligne peut-il utiliser ?
En outre, des données bancaires telles qu'un n° de carte bancaire.

1.4. Peut-on librement mettre en ligne un site de vente en ligne ? Justifier.
Préalablement à la mise en ligne d'un site e-commerce, il faut accomplir une formalité déclarative auprès de la CNIL. Du moins, jusqu'en 2018 (règlement européen RGPD : Réglementation Générale sur la Protection des Données), il fallait accomplir une déclaration simplifiée auprès de la CNIL.

1.5. A quelles sanctions s'expose une personne ne respectant pas la Loi Informatique et Libertés ?
Jusqu'à 5 ans d'emprisonnement et 150000€ d'amendes, 300000€ en cas de récidive.

La diffusion de contenus sur les réseaux sociaux (exemple : facebook, twitter…) ou plus généralement sur des logiciels utilisant des outils d'intelligence artificielle (exemple : gmail, facebook, twitter…) n'est pas forcément si anodine…

1.6. A votre avis, quel est le risque de diffuser des informations sur pareils logiciels ?
Les réseaux sociaux collectent de multiples informations personnelles. On peut craindre qu'ils utilisent ces données à des fins commerciales ou encore, éventuellement, aux fins de dresser des profils psychologiques des individus.

2. Sécurité des données et des échanges

Il existe de nombreuses techniques de piratage poursuivant divers objectifs : intercepter des communications, voler des mots passe ou des informations sensibles, voler des données de valeur… Dès lors, il importe de veiller à la sécurité des informations et des échanges de manière proportionnée.

Ainsi, on peut fournir des recommandations parmi lesquelles :
- Utiliser des mots de passe fiables ;
- Ne payer en ligne que sur des sites sécurisés (HTTPS) ;
- Ne jamais divulguer ou « laisser trainer » ses mots de passe ;
- Etc.

Tout d'abord, qu'est-ce qu'un mot de passe fiable ? Un mot de passe fiable est un mot de passe qui n'est pas sensible au *brute forcing* (force brute). L'attaque par force brute (*brute-force attack* ou plus simplement *brute forcing*) est un type d'attaque consistant à tester des combinaisons jusqu'à trouver la bonne. A titre informel, une variante du *brute forcing* classique, beaucoup plus efficace, est l'attaque par dictionnaire.

2.1. En supposant qu'un mot de passe est constitué de 3 caractères pouvant être un « 0 » ou un « 1 », énumérer les mots de passe possibles. Combien y a-t-il de possibilités ?

Les mots de passe possibles sont : 000, 001, 010, 011, 100, 101, 110, 111, soit 8 possibilités.

2.2. En supposant maintenant qu'un mot de passe est constitué d'au maximum 3 caractères pouvant être un « 0 » ou un « 1 », énumérer les mots de passe possibles. Combien y a-t-il de possibilités ?

Les mots de passe possibles sont : 0, 1, 00, 01, 10, 11 ainsi que les 8 possibilités précédentes, soit 8 + 4 + 2 = 14 possibilités (= 2^3+2^2+2).

2.3. On note a le nombre de caractères possibles et n le nombre de caractères maximum composant le mot de passe. En vous servant de la question précédente, déterminer NB, NB étant le nombre de possibilités de mots de passe en fonction de a et n.

NB = $a^n+a^{n-1}+\ldots+a \approx a^n$ (environ égal à a^n)

2.4. En déduire le nombre de mots de passe possibles si la longueur maximum du mot de passe est de 5 caractères pouvant être n'importe quel chiffre.

NB = $10^5+10^4+10^3+10^2+10^1$= 111 110

2.5. Quel est le nombre de mots de passe possibles si la longueur maximum du mot de passe est de 5 caractères pouvant être un chiffre, une lettre minuscule ou une lettre majuscule.

a = 10 + 26 + 26 = 62

NB = $62^5+62^4+62^3+62^2+62^1$ = 931 151 402

2.6. Calculer le nombre de mots de passe possibles dans les cas suivants :

Longueur maximum	Types de caractères	Nombre de possibilités	Temps de brute forcing
5	Chiffres, minuscules majuscules	931 151 402	≈ 93s ≈ 1min30
10	Chiffres, minuscules, majuscules	≈850 000 000 000 000 000 = 850 billiards	≈ 85 000 000 000s ≈ 2693 ans ≈ 27 siècles

Un ordinateur pour particulier relativement puissant peut approximativement tester 10 millions de possibilités par seconde. S'il y a 10 millions de mots de passe possibles, un tel ordinateur pourra par conséquent potentiellement pirater le mot de passe en 1 seconde.

2.7. En partant de l'hypothèse ci-dessus, compléter la colonne « Temps de brute forcing » du précédent tableau. Dans cette colonne, on indiquera le temps qu'il faut pour pirater un mot de passe en utilisant une attaque par force brute consistant à tester toutes les combinaisons possibles.

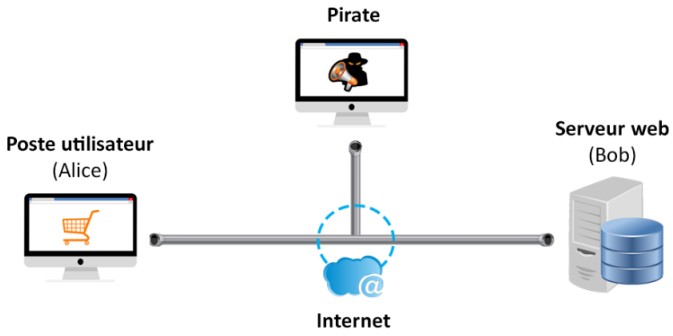
Voir tableau ci-dessus.

En pratique, il est recommandé de ne pas stocker en clair (non crypté) les mots de passe des utilisateurs au sein d'une base de données. On préfère stocker « l'empreinte numérique » du mot de passe, qu'on appelle aussi le « haché ». Cette empreinte est calculée grâce à une fonction de hachage, non inversible, qui retourne une valeur de taille fixe. Deux mots de passe ou messages différents ont une empreinte différente.

2.8. Quel est le risque lié au stockage des mots de passe en clair en base de données ?

Toute personne qui a accès à la base de données pourrait connaître le mot de passe des utilisateurs ce qui est anormal dans la mesure où un mot de passe est une information personnelle et confidentielle.

2.9. En quoi l'utilisation du hachage prévient-il ce risque ?
Comme la fonction de hachage est non inversible, on ne pourra pas retrouver le mot de passe à partir de son empreinte numérique. Le mot de passe reste donc confidentiel.



Le piratage de mot de passe vise de manière générale au piratage de comptes utilisateurs. Il ne constitue néanmoins pas le seul risque de sécurité en matière d'information et d'échanges d'informations. Un autre risque est celui de l'interception de communication. Intercepter une communication, c'est pour un pirate capter les informations résultant des échanges distants entre deux utilisateurs. L'interception de communication est un risque dès lors que des informations sensibles ou confidentielles sont échangées. Explication de l'illustration ci-dessus :

- A partir de son poste informatique, Alice se connecte sur le site e-commerce Bob.
- Alice et Bob échangent donc des messages (requêtes et réponses HTTP, cf. *Cours Q3 - web et PHP*).
- Le pirate intercepte tous les messages échangés.
- Par conséquent, si la communication n'est pas cryptée, le pirate va pouvoir très clairement lire le contenu de tous les messages. C'est pourquoi il convient de crypter/chiffrer la communication. On parle de canal crypté, c'est-à-dire que les messages sont cryptés.

Un algorithme de cryptage/chiffrement nécessite une clé de cryptage. C'est cette clef de cryptage qui va servir à crypter les messages échangés. De manière très générale, il existe deux formes de cryptage :

- Le **cryptage symétrique** : la clef de cryptage est partagée par Alice et Bob. Elle sera tout à la fois à crypter et à décrypter les messages. Le problème ? Alice et Bob doivent au préalable s'échanger les clefs. Alors, le pirate peut se faire passer pour Bob auprès d'Alice et pour Alice auprès de Bob (usurpation d'identité). Cette forme de piratage est appelée attaque du *man in the middle* (l'homme au milieu).

- Le **cryptage asymétrique** : la clef de cryptage est constituée d'une clef publique et d'une clef privée. Bob transmet à Alice sa clef publique. Elle permet à Alice de crypter les messages qu'elle transmet à Bob. Bob peut décrypter les messages cryptés grâce à la clef privée, que seul lui connaît. Le problème ? Une fois encore, le pirate peut usurper l'identité d'Alice et Bob. Pour contrer le problème, on utilise des **certificats d'authenticité** qui permettent de vérifier que la clef publique appartient bien à la bonne personne, ici Bob.

Etudions ensemble un algorithme de cryptage simple. Cet algorithme n'est pas fiable mais c'est un premier pas ! Il s'agit d'un algorithme de cryptage symétrique. L'algorithme que nous allons appliquer est le cryptage par substitution, aussi appelé cryptage César, ce dernier l'ayant utilisé pour crypter manuellement ses propres messages à l'époque romaine. La clef de cryptage de cet algorithme est un nombre entier.

Le principe de l'algorithme de cryptage par substitution est le suivant :

On associe un nombre à un caractère :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	!			
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37		

+5 (de N à S)

+5 (de U à Z)

Espace

- On se donne une clef de cryptage comprise entre 0 et le nombre de caractères, soit ici entre 0 inclus et 38 exclus, par exemple : $N = 5$
- On prend son message, par exemple : « UN MESSAGE CRYPTE »
- On va crypter un-à-un chacun des caractères du message en décalant chacun d'entre eux d'exactement N caractères.

U	N		M	E	S	S	A	G	E		C	R	Y	P	T	E	
20	13	37	12	4	18	18	0	6	4	37	2	17	24	15	19	4	*Message en clair*
25	18	4	17	9	23	23	5	11	9	4	7	22	29	20	24	9	*Message crypté*
Z	S	E	12	J	X	X	F	L	J	E	H	W	3	U	Y	J	

- Pour décrypter le message, on procèdera en sens inverse, c'est-à-dire qu'on effectue les mêmes calculs, mais avec la clef inverse, soit ici : $N = -5$ ou $N = 38 - 5 = 33$

2.10. Crypter le message suivant avec la clef $N = 7$: « IL ETAIT UNE FOIS »

I	L		E	T	A	I	T		U	N	E		F	O	I	S			
8	11	37	4	19	0	8	19	37	20	13	4	37	5	14	8	18			
15	18	6	11	26	7	15	26	6	27	20	11	6	12	21	15	25			
P	S	G	L	0	H	P	0	G	1	U	L	G	M	V	P	Z			

2.11. Décrypter le message suivant, lequel a été crypté avec la clef $N = 9$: « KJLLJUJ30NJ2H »

K	J	L	L	J	U	J	3	0	N	J	2	H							
10	9	11	11	9	20	9	29	26	13	9	28	7							
1	0	2	2	0	11	0	20	17	4	0	19	36							
B	A	C	C	A	L	A	U	R	E	A	T	!							