Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
- Sécurité des systèmes
- Codes malveillants et outils de sécurité

II. Sécurité dans le code

III. Sécurité des réseaux

- Bases de la sécurité des réseaux

IV. Sécurité des réseaux sans fil

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - Enjeux et objectifs de la sécurité
  - Gestion de risques
  - Principes généraux des méthodes de sécurité informatique
  - Les méthodes de sécurité informatique
  - Introduction à la cryptologie
  - Notions fondamentales (histoire, principe de Kerckhoffs, vocabulaire)
  - Cryptographie symétrique et asymétrique
  - Signature numérique
  - Confiance en une clé publique
  - Infrastructure de gestion de clés (PKI)

- Sécurité des systèmes
  - Contrôle d'accès
  - Sécurité des systèmes d'exploitation

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Codes malveillants et outils de sécurité
  - Codes malveillants, Virus, Ver, Cheval de Troie, Spyware, Rootkit, Hypervirus
  - Moyens de prévention
  - Outils de sécurité
  - Antivirus
  - Antispyware
  - Scanners de vulnérabilité
  - Gestion de la sécurité
  - Patch management
  - Chiffrement de fichiers

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Enjeux et objectifs de la sécurité**

    - ❑ **Place du système d'information dans l'entreprise**
    - ❑ **L'information est une ressource stratégique**
    - ❑ **Le système d'information facteur d'amélioration de la compétitivité**

    - ❑ **Maintien de la disponibilité**
    - ❑ **Intégrité**
    - ❑ **Confidentialité**

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Gestion de risques**

❑Deux thermes utilisés par les spécialistes

❖Sécurité-innocuité : Pour les nuisances de nature aléatoire (les dangers)

Elle concerne l'aptitude du système à ne pas connaître d'événements catastrophiques :

a) Dangers matériels
b) Dangers logiciels
c) Dangers de mauvaises interactions matériel / logiciel
d) Dangers humains non intentionnels

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Gestion de risques**

❑Deux thermes utilisés par les spécialistes

❖Sécurité-confidentialité : Pour les nuisances de nature volontaire (les menaces)

Elle concerne l'aptitude du système à se prémunir de la manipulation non autorisée de l'information à des fins malveillantes.

a) Menace stratégique

b) Menace terroriste

c) Menaces ludique

d) Menace mercantile

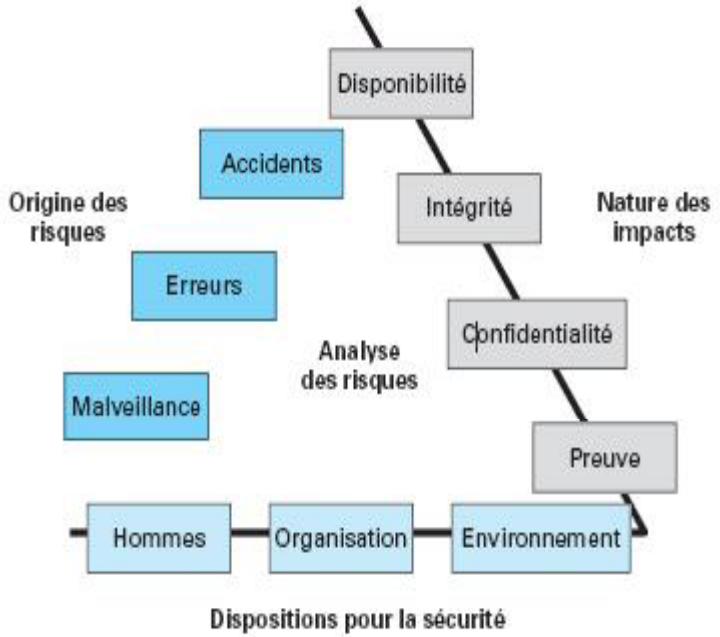
Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Principes généraux des méthodes de sécurité informatique**

Principes

Ils sont basés sur l'analyse des risques des systèmes informatiques



Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Principes généraux des méthodes de sécurité informatique**

❑Méthodes

Elles procèdent en plusieurs étapes.

❖Déterminer le périmètre du système

L'analyse doit couvrir tous les éléments qui peuvent contribuer à générer des défaillances (environnement, matériel, logiciel, application, réseau, exploitation).

❖Analyser les risques

L'évaluation du risque doit être effectuée en fonction de la durée et de la nature des pertes d'information.

❖Analyser les vulnérabilités

Elle doit couvrir tous les objets de l'environnement en relation avec le système d'information.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Principes généraux des méthodes de sécurité informatique**

❑ **Méthodes**

Elles procèdent en plusieurs étapes.

❖ **Identifier les dispositions à prendre**

Les dispositions sont orientées vers la disponibilité (reprise rapide, passage en mode dégradé) ou vers le secours (restauration des données, restauration de l'infrastructure).

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode Marion

La méthode Marion (Méthode d'analyse de risques informatiques optimisée par niveau) a été conçue par le Clusif (Club de la sécurité des systèmes d'information français)en 1983.

Cette méthode repose sur les six principes de base suivants :

a) ***Sensibilisation à fin d'avoir une forte implication de la direction général à l'utilisateur final.***

b) ***Réduction des vulnérabilités dues aux menaces et dangers, et ayant un impact sur la disponibilité, l'intégrité ou la confidentialité des données.***

c) ***Spécifications des solutions fournies à chaque entreprise.***

d) ***Distinction entre les différents niveaux de risques.***

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode Marion

e) Choix des moyens de sécurité en fonction de la priorité des moyens de protection vis-à-vis des moyens de prévention et sur l'optimisation du rapport qualité/coût

f) Quantification préalable de toutes les informations dans le schéma directeur de la sécurité du système d'information.

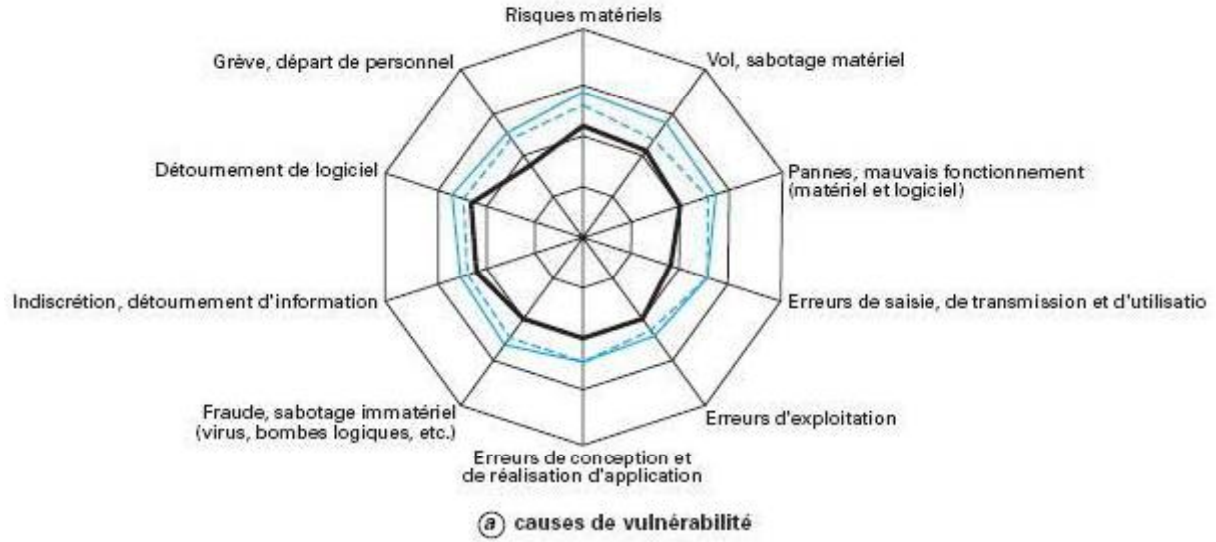
Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode Mehari

En 1997, le Clusif a évolué de la méthode Marion à la méthode Mehari (Méthode harmonisée d'analyse des risques). La nouvelle méthode était revendiquée comme étant plus cohérente et offrant une mesure de l'évaluation des risques.



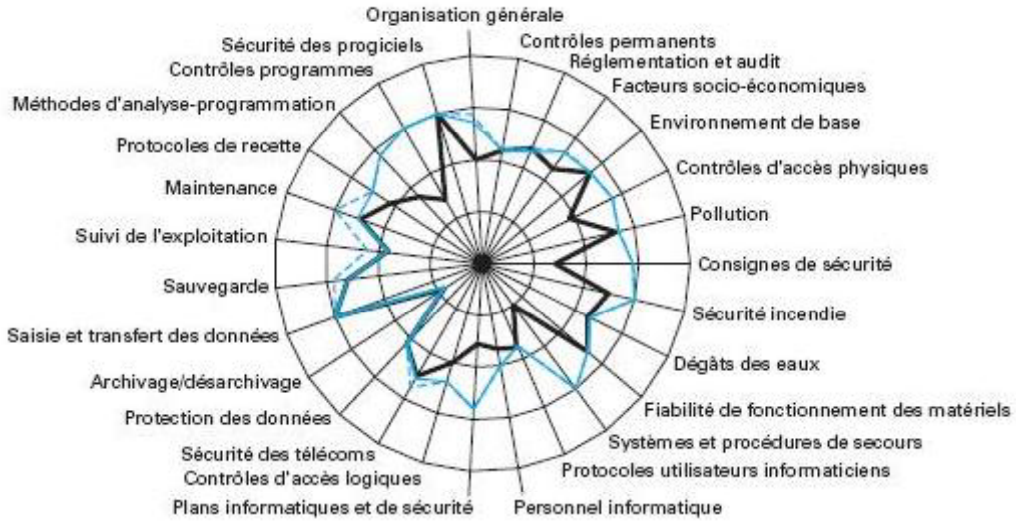
ⓐ causes de vulnérabilité

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode Mehari



ⓑ facteurs de risques

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

Méthode Mehari

La méthode Mehari s'appuie sur :

a) ***Un plan stratégique de sécurité (PSS) qui fixe les objectifs de sécurité et qui qualifie le niveau de gravité des risques encourus .***

b) ***Des plans opérationnels de sécurité (POS) qui déterminent, par site ou par entité géographique, les mesures de sécurité à mettre en place, tout en assurant la cohérence des actions choisies.***

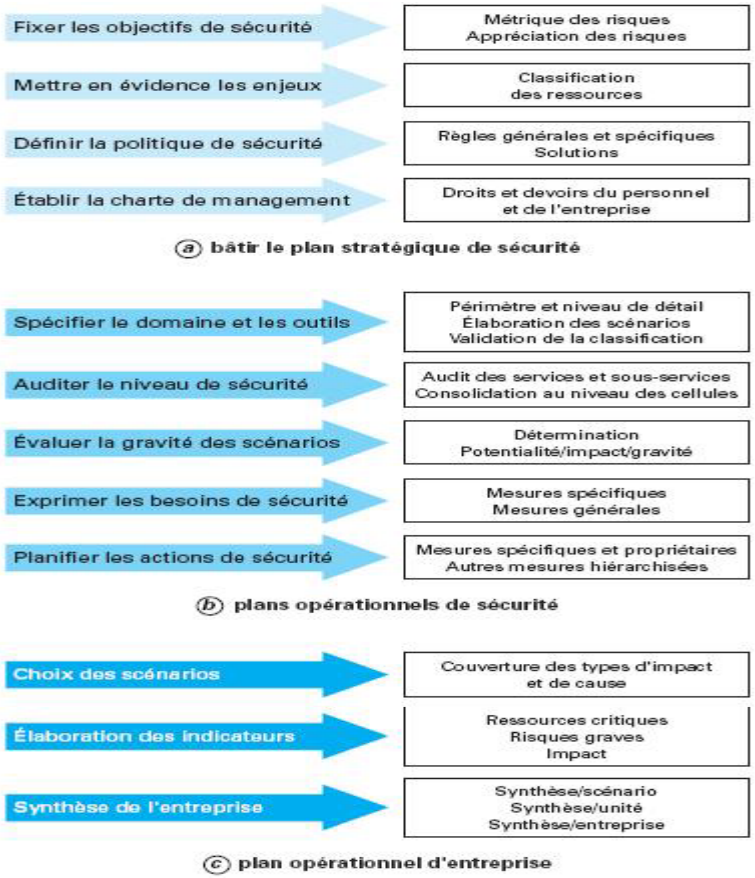
c) ***Un plan opérationnel d'entreprise (POE) qui permet le pilotage de la sécurité au niveau stratégique par la mise en place d'indicateurs et la remontée d'informations sur les scénarios les plus critiques.***

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode Mehari



Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode EBIOS

EBIOS (méthode pour l'expression des besoins et l'identification des objectifs de sécurité) est une méthode basée sur l'analyse des risques, elle est apparue dans sa première version en 1995 et elle a été élaborée par la DCSSI en France.
La méthode EBIOS permet l'expression :

a) ***Des besoins de sécurité.***

b) ***L'identification des objectifs de sécurité pour un système à concevoir ou un système existant.***

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode EBIOS

La méthode EBIOS comprend quatre étapes:

a) Étude de contexte :
cette première étape permet de prendre connaissance du domaine et de le modéliser.

b) Expression des besoins intrinsèques de sécurité :
les besoins essentiels de sécurité doivent être issus des exigences opérationnelles du système indépendamment de toute solution technique.

c) Étude des risques :
De manière classique, cette étude passe par les étapes suivantes : sélection des menaces, détermination des vulnérabilités, association des menaces et des vulnérabilités en termes de risques.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode EBIOS

d) Identification des objectifs de sécurité déduits de :
La confrontation des risques spécifiques aux besoins de sécurité .
La prise en compte des contraintes (en particulier la réglementation).
L'application de la politique de sécurité retenue pour les informations.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode OCTAVE / OCTAVE-S (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Une méthode d'évaluation des vulnérabilités, des menaces, et des actifs opérationnels critiques publiée par le SEI ,(Software Engineering Institute) de la Carnegie Mellon University , université américaine située à Pittsburgh très reconnue dans le domaine de la sécurité.

La première version d'OCTAVE est parue en 1999. En version 2.0 depuis 2001, la méthode a été déclinée en une version pour les PME en 2003 en finalisation « OCTAVE-S ». L'ensemble de la méthode est publique et maintenue par l'université.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode OCTAVE / OCTAVE-S

L'approche OCTAVE est avant tout basée sur les actifs de l'entreprise. L'équipe d'analyse devra donc :

a) Identifier les actifs importants de l'entreprise.

b) Centrer son analyse des risques sur ces actifs les plus critiques.

c) Considérer les relations entre ces actifs ainsi que les menaces et les vulnérabilités pesant sur eux.

d) Evaluer les risques d'un point de vue opérationnel.

e) Créer une stratégie de protection basée sur des pratiques.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode OCTAVE / OCTAVE-S

a) ***Phase1:***

C'est une évaluation avant tout organisationnelle.

- ***L'identification des ressources informatiques importantes.***
- ***Les menaces associées et les exigences de sécurité qui leur sont associées.***
- ***Evaluation des pratiques actuelles de l'organisation pour protéger ces ressources critiques (si elles existent) .***
- ***Identification des vulnérabilités sur ces ressources.***
- ***Etude des menaces, et qui pourrait les exploiter pour dégager ensuite un profil de menace.***

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode OCTAVE / OCTAVE-S

b) Phase2: Identification des vulnérabilités de l'infrastructure

C'est une évaluation de l'infrastructure informatique.

- ***Identification des moyens d'accès.***
- ***Regroupement par classe des composants qui sont reliés à ces moyens d'accès.***
- ***Détermination des classes résistantes aux attaques .***

c) Phase3: développement de la stratégie de sécurité et planification

L'équipe d'analyse procèdera à une analyse des risques sur les actifs opérationnels et comment les traiter. Elle produira plusieurs documents.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑ **Méthode OCTAVE / OCTAVE-S**

La méthode OCTAVE se décompose en 8 processus répartis dans les 3 phases majeures de la méthode.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

Méthode OCTAVE / OCTAVE-S

	PHASE	PROCESSUS
OCTAVE	Vue Organisationnelle	Identification des connaissances par les cadres Supérieurs
		Identification des connaissances par les cadres de l'opérationnel
		Identification des connaissances par les équipes de production
		Création des profils de menace
	Vue technique	Identification des composants clefs
		Evaluation des composants sélectionnés
	Développement	Analyse des risques
		Développements

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

Méthode OCTAVE / OCTAVE-S

	PHASE	PROCESSUS
OCTAVE-S	Vue Organisationnelle	Dégager des informations sur l'organisation
		Créer les profils de menace
	Vue technique	Examiner l'infrastructure informatique en relation avec les actifs critiques
	Développement	Identifier et analyser les risques
		Développer la stratégie de protection et les plans de réduction des risques

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

Méthode ITBPM (IT Baseline Protection Manual)

L'ITBPM est l'oeuvre du bureau allemand pour la sécurité informatique (Bündesamt für Sicherheit in der Informationstchnik – BSI).

ITBPM utilise une toute autre approche en partant du principe que la procédure de sécurité est souvent longue, coûteuse, et que ce sont la plupart du temps les mêmes types de ressources qui doivent être protégés. Donc, Seulement celles qui requièrent un niveau de sécurité supérieur doivent subir une analyse approfondie.

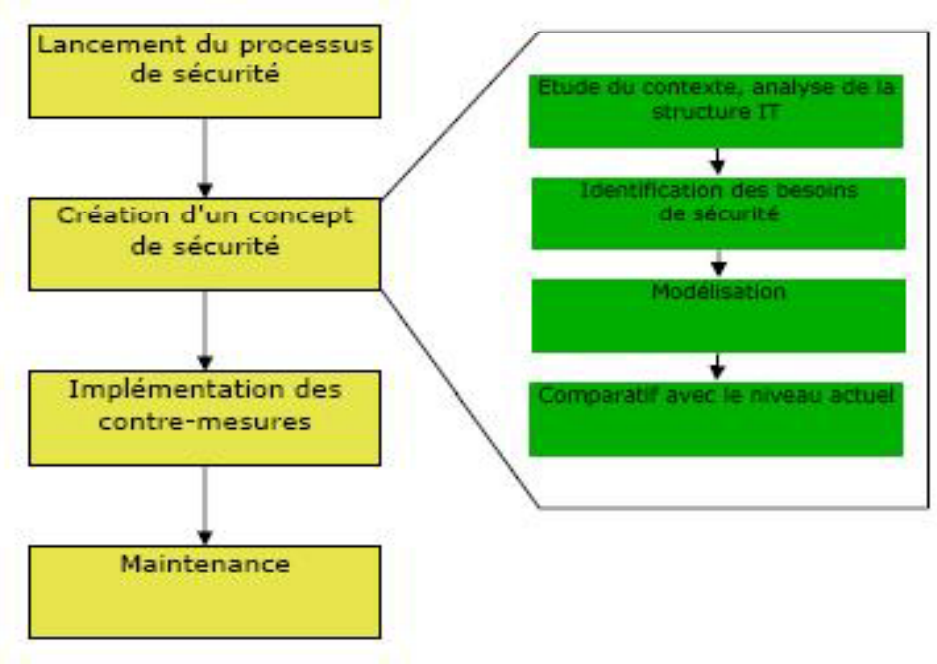
Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

Méthode ITBPM (IT Baseline Protection Manual)

ITBPM suggère d'aborder la sécurité dans une organisation comme un processus composé de plusieurs phases.



Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

Méthode ITBPM (IT Baseline Protection Manual)

Une organisation, et en particulier ses actifs informatiques, peut être décomposée en plus petites entités selon leur nature. Ces entités, l'ITBPM les nomme modules.

ITBPM recense 7 types de modules :

a) ***Les modules transversaux à toute l'organisation (Personnel, données personnelles, reprise après incident…)***

b) ***Les modules d'infrastructure (Câbles, locaux, armoires…)***

c) ***Les modules concernant les systèmes non connectés (Machines non reliées à un réseau…)***

d) ***Les modules concernant les systèmes connectés(Machines reliées à un réseau sur l'extérieur…)***

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode ITBPM (IT Baseline Protection Manual)

e) Les modules concernant les systèmes de transmission de données (Modems, firewalls, serveurs mail)

f) Les modules télécommunications (PBX, Téléphones mobiles, point de présence)

g) Divers (Bases de données, archivage…)

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑ **Méthode ITBPM (IT Baseline Protection Manual)**

La méthode ITBPM peut répondre aux menaces par 6 contre-mesures:

a) ***Les mesures d'infrastructure***
Ce sont toutes les mesures qui sont mises en place au niveau des bâtiments et du monde physique.

b) ***Les mesures organisationnelles***
Ce sont les dispositions qui mettent en place généralement des procédures spécifiques.

c) ***Les mesures humaines***
On retrouvera dans cette catégorie tout ce qui a trait au personnel et en particulier à sa formation.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode ITBPM (IT Baseline Protection Manual)

e) Les mesures matérielles et logicielles

f) Les mesures sur télécommunications

Ces 2 catégories sont difficilement dissociables car elles regroupent toutes les mesures techniques : authentification, configuration, moyens de protection contre les virus…

g) Les mesures de réponse sur incident

Toutes les mesures pour éviter de perdre son travail et assurer la continuité du « business ».

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑ **Méthode ITBPM (IT Baseline Protection Manual)**

La méthode ITBPM est accompagnée d'un guide qui comporte une liste de 50 mesures essentielles que devraient mettre en place toute organisation.

a) Approche de la sécurité

1. *Considérer la sécurité dès le départ des projets*
2. *Lorsque les ressources manquent, pensez à d'autres approches*
3. *Des objectifs de sécurité doivent être définis en fonction des besoins*
4. *Des contrôles des objectifs de sécurité doivent être définis*
5. *Un plan d'action doit être défini*
6. *Les mesures de sécurité particulièrement onéreuses doivent être évitées*
7. *Définir les responsabilités*
8. *Les politiques de sécurité et les responsabilités doivent être communiquées*
9. *Vérifier régulièrement le niveau de sécurité*
10. *Les mesures de sécurité doivent être contrôlées régulièrement*
11. *Une gestion complète de la sécurité doit être envisagée à long terme*
12. *La politique de sécurité doit être clairement formalisée*

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode ITBPM (IT Baseline Protection Manual)

b) Sécurité des systèmes

13. Les protections existantes doivent être utilisées
14. L'antivirus doit être utilisé à travers toute l'organisation
15. L'accès aux données doit être restreint au strict minimum
16. Des rôles et des profils doivent être assignés à tous les utilisateurs
17. Les privilèges de l'administrateur doivent être restreints également
18. Les droits des applications doivent être restreints
19. Les configurations par défaut doivent être modifiées
20. Les notices et mode d'emploi doivent être lues
21. Une documentation sur l'installation et le fonctionnement des systèmes est nécessaire
22. Les réseaux doivent être protégés par un firewall
23. Un firewall doit satisfaire certaines spécifications

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

Méthode ITBPM (IT Baseline Protection Manual)

24. Les données accessibles aux externes doivent être réduits au minimum
25. Les services et applications accessibles aux externes doivent être réduites au minimum
26. L'utilisation des navigateurs web est dangereuse
27. Attention aux pièces jointes
28. Un PC dédié pour Internet est la solution la moins onéreuse

c) Le facteur Homme

29. La politique de sécurité et les recommandations doivent être suivies
30.Ordre et propreté doivent régner sur les bureaux et aucune information sensible librement accessible
31.Des précautions particulières doivent être prises lors des travaux de maintenance

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑Méthode ITBPM (IT Baseline Protection Manual)

d) Maintenance des systèmes

37. Les mises à jour de sécurité doivent être régulièrement installées
38. Une veille technologie sur le matériel en place est nécessaire
39. Un plan d'action pour les mises à jour est nécessaire
40. Les migrations doivent faire l'objet de tests

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

Méthode ITBPM (IT Baseline Protection Manual)

e) Mécanisme de sécurité

41. Les mécanismes de sécurité doivent être employés avec précaution
42. Les mots de passe doivent être choisis de façon appropriée
43. Les mots de passe par défaut ou non défini doivent être remplacés
44. Les postes de travail doivent être verrouillés en l'absence de l'opérateur
45. Les données et systèmes sensibles doivent être protégés

f) Incidents

46. Des procédures d'urgence doivent être mises en place
47. Les données importantes doivent être sauvegardées
48. Les systèmes IT doivent être à l'abri du feu, de la chaleur, de l'eau et des coupures de courant
49. Des protections contre le vol et les intrus sont nécessaires
50. Un inventaire précis de ressources matérielles et logicielles doit être tenu

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑ **SSE-CMM / ISO 21827 (Systems Security Engineering-Capability Maturity Model)**

Initiative soutenue par la NSA datant d'avril 1993.

La première version du modèle apparut en octobre 1996 et la méthode d'évaluation en avril 1997.

Sa version 2 devenue la norme ISO 21827 en octobre 2002.

La version 3.0 du SSE-CMM est apparue en juin 2003 et constitue la dernière évolution en date.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑ **SSE-CMM / ISO 21827 (Systems Security Engineering-Capability Maturity Model)**

a) ***Objectifs***

SSE-CMM s'adresse à tout type et taille d'organisation, aussi bien commerciale que gouvernementale voire universitaire.
La norme peut s'appliquer également aux développeurs de produits sécurisés ou à l'implémentation de contre-mesures.

b) ***Concepts***

La méthode utilise une approche processus.
Le but du modèle est de pouvoir mesurer le degré de maturité des processus sécurité d'une entité.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑ **SSE-CMM / ISO 21827 (Systems Security Engineering-Capability Maturity Model)**

L'approche a deux dimensions « DOMAINE » et « ADAPTABILITE »

- *DOMAINE :*
  Représente les pratiques liées à la SSIC « pratiques de bases » (BP)
- *ADAPTABILITE:*
  Représente les pratiques liées à la gestion et à la mise en place de ces (BP). On les appellera « les pratiques génériques » (GP).

Exemple:

En SSIC l'une des tâches principales est l'identification des vulnérabilités. Cette activité est répertoriée dans SSE-CMM comme pratique de base. Une façon de déterminer la capacité d'une organisation de réaliser une tâche donnée est de vérifier qu'elle dispose d'un processus pour allouer des ressources à ces activités. Cette capacité est répertoriée dans SSE-CMM comme pratique générique.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑SSE-CMM / ISO 21827 (Systems Security Engineering-Capability Maturity Model)

c) BP & GP

La méthode répertorie ainsi 129 BP réparties en 22 catégories de processus.

- ***Les 11 catégories de processus spécifiques à la sécurité sont les suivants :***
  - ***Administrer les contre-mesures***
  - ***Evaluer les impacts***
  - ***Evaluer les risques***
  - ***Evaluer les menaces***
  - ***Evaluer les vulnérabilités***
  - ***Respect des exigences d'assurance***
  - ***Coordonner la sécurité***
  - ***Surveiller l'état de la sécurité***
  - ***Fournir des informations sur la sécurité***
  - ***Spécifier les besoins de sécurité***
  - ***Vérifier et valider la sécurité***

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑ **SSE-CMM / ISO 21827 (Systems Security Engineering-Capability Maturity Model)**

- *Les 11 autres catégories liées à la gestion de l'organisation :*
  - *Assurer la qualité*
  - *Gérer la configuration*
  - *Gérer les risques du projet*
  - *Surveiller et contrôler l'effort technique*
  - *Planifier l'effort technique*
  - *Définir les processus de l'organisation*
  - *Améliorer les processus de l'organisation*
  - *Gérer l'évolution des produits*
  - *Gérer le support*
  - *Transférer les compétences et les connaissances*
  - *Se coordonner avec les fournisseurs*

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑SSE-CMM / ISO 21827 (Systems Security Engineering-Capability Maturity Model)

c) Approche propre de la sécurité

SSE-CMM divise la sécurité en 3 secteurs de base :

- ***Les risques***

  Risques = Menaces * Vulnérabilités * Impacts

  les groupes de BP sont :
  - ***PA02 Evaluer les impacts***
  - ***PA03 Evaluer les risques***
  - ***PA04 Evaluer les menaces***
  - ***PA05 Evaluer les vulnérabilités***

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

SSE-CMM / ISO 21827 (Systems Security Engineering-Capability Maturity Model)

- ***L'ingénierie***
  En utilisant divers documents tels que l'analyse des risques ou le cahier des charges, les spécialistes peuvent intégrer la sécurité dans leurs produits.

  Les 5 groupes de BP suivants sont dédiés à cette tâche :
  - ***PA01 Administrer les contre-mesures***
  - ***PA07 Coordonner la sécurité***
  - ***PA08 Surveiller l'état de la sécurité***
  - ***PA09 Fournir des informations sur la sécurité***
  - ***PA10 Spécifier les besoins de sécurité***

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Les méthodes de sécurité informatique**

❑ **SSE-CMM / ISO 21827 (Systems Security Engineering-Capability Maturity Model)**

- *L'assurance*

  Les exigences d'assurance sont souvent communiquées via un argument d'assurance, argument construit autour d'engagements à propos du système, eux-mêmes reposant sur des preuves.

  Les 2 BP restants sont concernés :
  - ***Expression des exigences d'assurance***
  - ***Vérifier et valider la sécurité***

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Histoire

l'histoire de la cryptographie est déjà longue. On rapporte son utilisation en Egypte il y a 4000 ans.

Sa mise en œuvre était limité aux besoins de l'armée et de la diplomatie.

La prolifération des systèmes de communication a fait sortir la cryptographie du domaine militaire.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Définitions

Cryptologie = Cryptographie + Cryptanalyse

❖Cryptologie

Une science mathématique qui comporte deux branches : la cryptographie et la cryptanalyse.

❖Cryptographie

Traditionnellement , c'est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées algorithmes cryptographiques, qui dépendent d'un paramètre appelé clef.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Définitions

Elle est composée de deux procédés:

a) Le chiffrement:

Afin de protéger un message , on lui applique une transformation qui le rend incompréhensible, et à partir d'un texte clair , on aura un texte chiffré ou cryptogramme.

b) Le déchiffrement:

Il permet de reconstruire le texte en clair à partir de texte chiffré.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Définitions

❖Cryptanalyse

C'est l'étude des procédés cryptographiques dans le but de trouver des faiblesses et, en particulier, de pouvoir décrypter des textes chiffrés.

❖Le décryptement:

C'est l'action consistant à retrouver le texte en clair sans connaître la clef de déchiffrement.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Définitions

❖Cryptosystème

Il est constitué d'un algorithme cryptographique ainsi que toutes les clés possibles et tous les protocoles qui le font fonctionner.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑ Principe de Kerckhoffs

a) Biographie

Kerckhoffs est né à Nuth en Hollande et fut baptisé Jean-Guillaume-Hubert-Victor-Françoise-Alexandere-Auguste Kerckhoffs von Niuewenhof. Il raccourcit son nom par la suite et entama des études à l'Université de Liège, où il obtient le grade de Docteur en Lettres. Après une période où il enseigna en France et dans les Pays-Bas, il devint professeur d'allemand à l'École des Hautes Études Commerciales et à l'École Arago.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑ **Principe de Kerckhoffs**

b) *Principes:*

En janvier 1883, Auguste Kerckhoffs (1835 - 1903) posa les principes de la cyptographie moderne dans l'article "La cryptographie militaire" paru dans le "Journal des Sciences Militaires".

1. ***Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;***
2. ***Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;***
3. ***La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;***

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Principe de Kerckhoffs

4. *Il faut qu'il soit applicable à la correspondance télégraphique ;*
5. *Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;*
6. *Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.*

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑ **Principe fondamental de la cryptographie**

Les ensembles publics, connus de tout le monde, sont les suivants :

M : ensemble de symboles formant les messages clair,
C : ensemble de symboles formant les messages chiffrés,
K : ensemble des clés.

Ce qui doit être secret, c'est la paire des clés de chiffrement et de déchiffrement (e,d) où e est élément de K et d est élément de K.

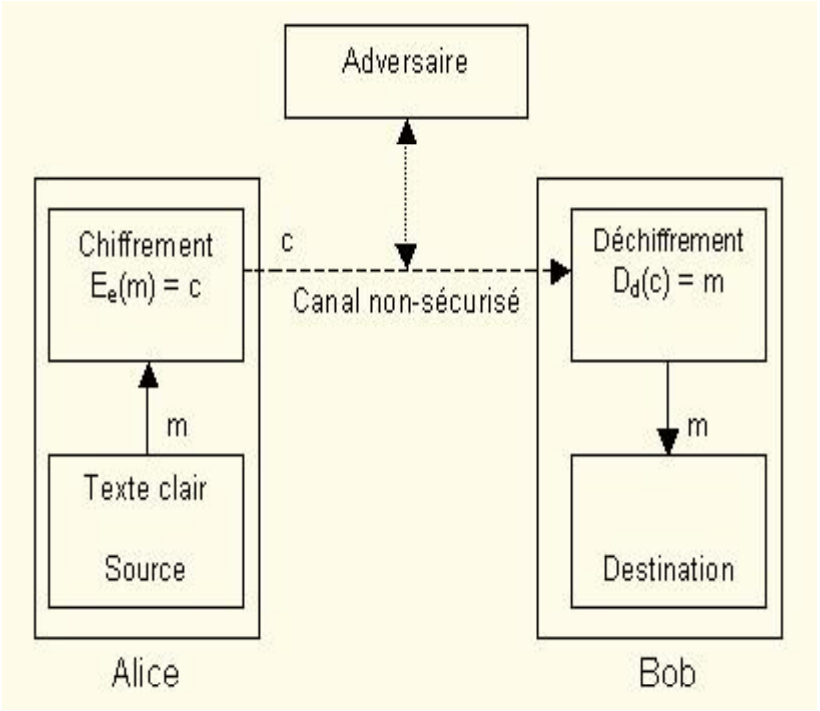
Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Principe de la cryptographie



Entité :
Quelqu'un ou quelque chose qui envoie, reçoit ou modifie de l'information. Elle peut être une personne physique ou morale, un ordinateur, etc. Alice et Bob sont des entités.

Expéditeur :
Entité qui envoie légitimement de l'information dans une transmission à deux parties. Alice est l'expéditrice.

Récepteur :
Entité destinée à recevoir l'information dans une transmission à deux parties. Bob est le récepteur.

Adversaire :
Entité qui n'est pas l'expéditeur ni le récepteur et qui tente de déjouer la sécurité d'une transmission à deux parties.

Canal :
Moyen de transport de l'information d'une entité à une autre.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑ But de la cryptographie moderne

Le but fondamental de la cryptographie est de respecter adéquatement les quatre objectifs majeurs de la sécurité, en théorie et en pratique :

a) Confidentialité

Assurer que les données concernées ne pourront être dévoilées qu'aux personnes autorisées.

b) Intégrité

Assurer que les données ne seront pas altérées pendant leur transmission ou leur stockage.

c) Authentification/identification

Prouver l'origine d'une donnée ou l'identité d'une personne.

d) Signature (proprement dite non-répudiation)

Permet à une personne à prendre part à un contrat avec impossibilité de renier ensuite ses engagements.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Objectifs de sécurité pour la cryptographie

a) ***Intimité et confidentialité***
Garder les informations secrètes de tous sauf les personnes autorisées à les voir.

b) ***Intégralité des informations***
Assurer que les informations n'ont pas été altérées par des personnes pas autorisées ou inconnues.

c) ***Authentification ou identification d'entité***
La confirmation de l'identité d'une entité.

d) ***Message d'authentification***
La confirmation de la source de l'information.

e) ***Signature***
Les moyens de lier l'information à une entité.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Objectifs de sécurité pour la cryptographie

f) Autorisation

Le transfert de la sanction officielle à une autre entité, à faire ou être quelque chose.

g) Validation

Les moyens de fournir l'autorisation d'utiliser ou de manipuler des informations.

h) Contrôle d'accès

Limiter l'accès des ressources aux personnes privilégiées.

i) Certification

L'approbation de l'information par une entité de confiance.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑ **Objectifs de sécurité pour la cryptographie**

j) Inclusion du temps
L'enregistrement du temps de création et d'existence de l'information.

k) Vérification des témoins
La vérification de la création ou de l'existence de l'information par une entité autre que son créateur.

l) Réception
Approuver la réception de l'information.

m) Confirmation
Approuver que le service ait été fourni.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Introduction à la cryptologie**

❑Objectifs de sécurité pour la cryptographie

m) ***Confirmation***
Approuver que le service ait été fourni.

n) ***Propriété***
Les moyens de fournir à une entité le droit d'utiliser ou de transférer une ressource à d'autres.

o) ***Anonymat***
Cacher l'identité d'une entité impliquée dans un processus.

p) ***Non-répudiation***
Empêcher le démenti d'engagements ou d'actions précédentes.

q) ***Révocation***
La rétraction d'une certification ou d'une autorisation.

Abdelouahed Ennibi
Email: ennibi@gmail.com

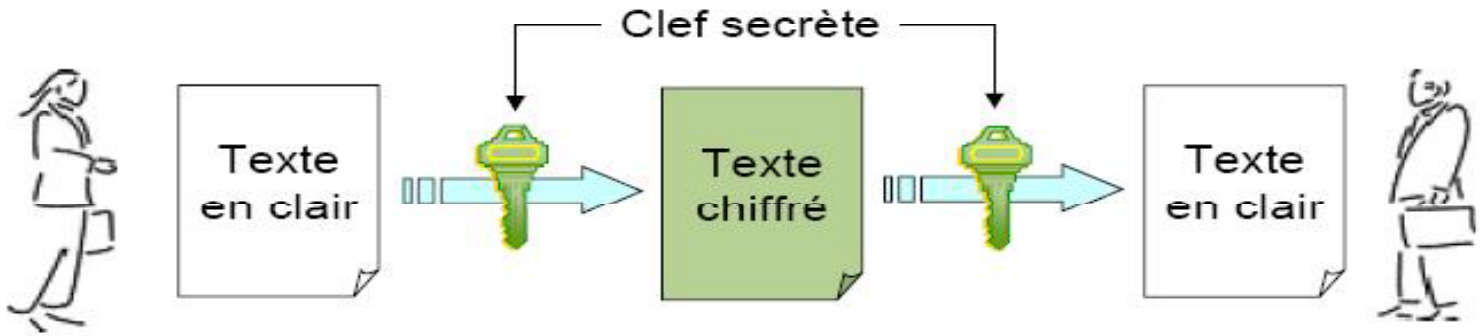
I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ **Système à clé privée**

Clef de chiffrement = Clef de déchiffrement

Dans la cryptographie conventionnelle ou à clef privée, les clefs de chiffrement ou déchiffrement sont identiques : c'est la clef secrète, qui doit être connue des tiers communicants et d'eux seuls. Le procédé de chiffrement est dit symétrique.



Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Chiffrement par blocs

Dans ce type de chiffrement, il y a une séparation du texte clair en blocs d'une longueur fixe, et un algorithme qui chiffre un bloc à la fois.

Une grandeur pertinente de la clé définie une bonne sécurité, car il faut considérer une recherche approfondie. Les clés très longues sont plus coûteuses en travail à cause notamment de leur génération, de leur transmission, de leur espace mémoire et de la difficulté de s'en rappeler (mots de passe).

La taille des blocs a un impact sur la sécurité et sur la complexité : les blocs de grandes dimensions sont plus sécuritaires mais sont plus lourds à implémenter.

Les chiffrements par blocs sont aussi utilisés dans des systèmes à clé publique.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Modes d'opérations du chiffrement par blocs

Il y a différentes méthodes d'utiliser les chiffrements par blocs, elles sont appelées « modes d'opération » (Anglais : modes of operation). Quatre modes sont définis dans FIPS 81 (Federal InformationProcessing Standards Publication 81, 2 décembre 1980) et aussi dans ANSI X3.106-1983 (American National Standards Institute).

Les quatre standards sont :

- **Electronic Code Book** (ECB),
- **Cipher Block Chaining** (CBC),
- **Cipher FeedBack** (CFB) et
- **Output FeedBack** (OFB).

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ Modes d'opérations du chiffrement par blocs

a) *Electronic Code Book (ECB)*

C'est la façon la plus évidente des modes d'opération, il applique simplement l'algorithme au texte clair en transformant normalement chaque bloc de texte clair.

Représentation :

T[n] = nième bloc de texte clair.
C[n] = nième bloc de texte chiffré.
E(m) = fonction de chiffrement du bloc m.
D(m) = fonction de déchiffrement du bloc m.

Chiffrement : C[n] = E(T[n])
Déchiffrement : T[n] = D(C[n])

Note : Ici T et C sont d'une longueur fixe.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ Modes d'opérations du chiffrement par blocs

Il y a deux problèmes relatifs à ce mode.

- *Le premier est que si on utilise deux fois le même texte clair et la même clé de chiffrement, le résultat du chiffrement sera identique.*
- *Le deuxième est qu'il faut un nombre d'octets de texte clair disponible (relatif à l'algorithme, huit octets pour le DES par exemple) avant de commencer le chiffrement.*

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Modes d'opérations du chiffrement par blocs

b) Cipher Block Chaining (CBC)

C'est un des modes les plus populaires. Il est une solution au premier problème du mode ECB. Avant d'être chiffré, l'opération binaire XOR est appliquée entre le bloc actuel de texte clair et le bloc précédent de texte chiffré. Pour le tout premier bloc, un bloc ayant un contenu aléatoire est généré et utilisé pour l'application de l'opération XOR, appelé « vecteur d'initialisation » (initialization vector). Ce premier bloc est envoyé tel quel avec le message chiffré.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Modes d'opérations du chiffrement par blocs

b) *Cipher Block Chaining (CBC)*

Représentation

T[n] = nième bloc de texte clair.
C[n] = nième bloc de texte chiffré.
E(m) = fonction de chiffrement du bloc m.
D(m) = fonction de déchiffrement du bloc m.
VI = vecteur d'initialisation
^ = OU-Exclusif
Chiffrement : C[0] = E(T[0] ^ VI)
C[n] = E(T[n] ^ C[n-1]) , si (n > 0)
Déchiffrement : T[0] = D(C[n]) ^ VI
T[n] = D[C[n]) ^ C[n-1] , si (n > 0)

Note : Ici T et C sont d'une longueur fixe.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ Modes d'opérations du chiffrement par blocs

c) *Cipher FeedBack (CFB)*

Le mode qui semble éviter tous les problèmes vus récemment est le CFB. L'opération XOR est appliquée entre le bloc de texte clair et le résultat précédent chiffré à nouveau par la fonction de chiffrement.
Pour le premier bloc de texte clair, on génère un vecteur d'initialisation.

Représentation

T[n] = nième bloc de texte clair.
C[n] = nième bloc de texte chiffré.
I[n] = nième bloc temporaire
E(m) = fonction de chiffrement et de déchiffrement du bloc m
VI = vecteur d'initialisation
^ = OU-Exclusif

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Modes d'opérations du chiffrement par blocs

c) *Cipher FeedBack (CFB)*

Chiffrement : I[0] = VI
I[n] = C[n-1] , si (n > 0)
C[n] = T[n] ^ E(I[n])

Déchiffrement : I[0] = VI
I[n] = C[n-1], si (n > 0)
T[n] = C[n] ^ E(I[n])

Note : Ici T et C sont d'une longueur fixe. La fonction de chiffrement et de déchiffrement est la même.

Le mode CFB offre une grande sécurité.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**
    - **Modes d'opérations du chiffrement par blocs**

d) Output FeedBack (OFB)

Le mode OFB est une solution aux deux problèmes relatifs au mode ECB. Au départ un vecteur d'initialisation est généré. Ce bloc est chiffré à plusieurs reprises et chacun des résultats est utilisé successivement dans l'application de l'opération XOR avec un bloc de texte clair. Le vecteur d'initialisation est envoyé tel quel avec le message chiffré.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Modes d'opérations du chiffrement par blocs

d) *Output FeedBack (OFB)*

Représentation

T[n] = nième bloc de texte clair.
C[n] = nième bloc de texte chiffré.
I[n] = nième bloc temporaire
R[n] = nième bloc temporaire second
E(m) = fonction de chiffrement et de déchiffrement du bloc m
VI = vecteur d'initialisation
^ = OU-Exclusif

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ Modes d'opérations du chiffrement par blocs

d) Output FeedBack (OFB)

Chiffrement : $I[0] = VI$
$I[n] = R[n-1]$, si $(n > 0)$
$R[n] = E(I[n])$
$C[n] = T[n] \wedge R[n]$

Déchiffrement : $I[0] = VI$
$I[n] = R[n-1]$, si $(n > 0)$
$R[n] = E(I[n])$
$T[n] = C[n] \wedge R[n]$

Note : Ici T et C sont d'une longueur fixe.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Modes d'opérations du chiffrement par blocs

d) Output FeedBack (OFB)

Ce mode a lui-même deux autres problèmes. Le texte clair est seulement soumis à un XOR. Si le texte clair est connu, un tout autre texte clair peut être substitué en inversant les bits du texte chiffré de la même manière qu'inverser les bits du texte clair (bit-flipping attack). De plus il y a une mince possibilité qu'une clé et un vecteur d'initialisation soient choisis tels que les blocs successifs générés puissent se répéter sur une courte boucle.
Le mode OFB est souvent utilisé comme générateur de nombre aléatoire.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ **Transformations du chiffrement par blocs**

a) *Chiffrement par substitution*

Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités. On distingue généralement plusieurs types de cryptosystèmes par substitution :

La substitution monoalphabétique consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet.

Exemple : le chiffre de Cesar

On décale les lettres de 3 positions

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
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

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ **Transformations du chiffrement par blocs**

a) *Chiffrement par substitution*

***La substitution polyalphabétique** consiste à utiliser une suite de chiffres monoalphabétique réutilisée périodiquement .*
Par exemple, on pourra utiliser n substitutions monoalphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texte en clair.

***Exemple :** le chiffre de Vigenere*

On prend les 26 chiffres de César.
Les chiffres associés aux 26 décalages possibles sont représentés par une lettre.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) *Chiffrement par substitution*

On peut résumer ces décalages avec un carré de Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) *Chiffrement par substitution*

Pour coder un message, on choisit une clé qui sera un mot de longueur arbitraire. On écrit ensuite cette clé sous le message à coder, en la répétant aussi souvent que nécessaire pour que sous chaque lettre du message à coder, on trouve une lettre de la clé. Pour coder, on regarde dans le tableau " carré de Vigenère" l'intersection de la ligne de la lettre à coder avec la colonne de la lettre de la clé.

Exemple :
On veut coder le texte "CRYPTOGRAPHIE DE VIGENERE" avec la clé "MATHWEB".
On commence par écrire la clef sous le texte à coder :

C	R	Y	P	T	O	G	R	A	P	H	I	E		D	E		V	I	G	E	N	E	R	E
M	A	T	H	W	E	B	M	A	T	H	W	E		B	M		A	T	H	W	E	B	M	A

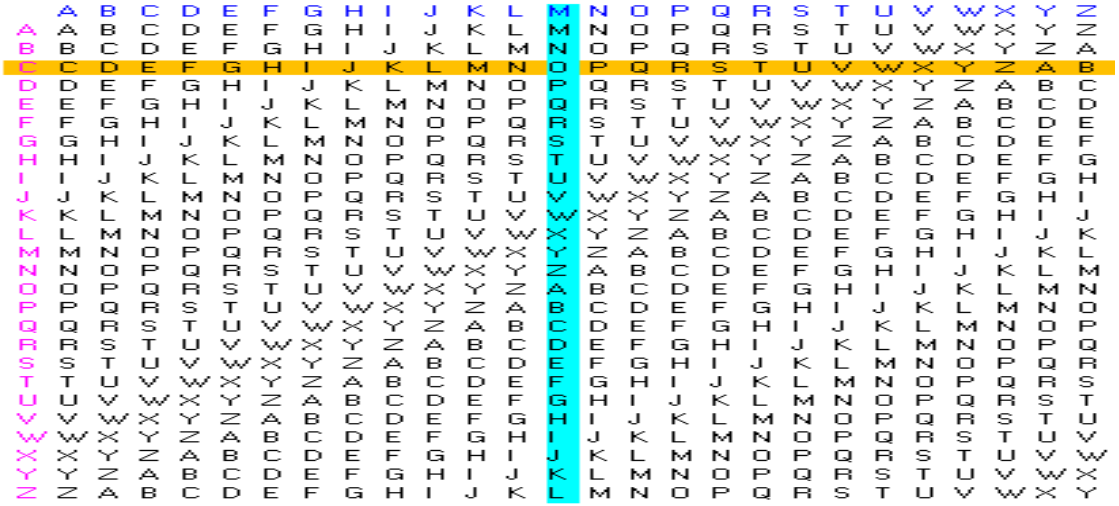
Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) *Chiffrement par substitution*



Pour coder la lettre C, la clé est donnée par la lettre M. On regarde dans le tableau l'intersection de la ligne donnée par le C, et de la colonne donnée par le M. On trouve O. Puis on continue. On trouve : ORRWPSHDAIOEI EQ VBNARFDE

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) *Chiffrement par substitution*

***La substitution homophonique** permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères.*
Même principe que le cryptage précédent si ce n'est que la transformation n'est plus bijective. Ainsi à une lettre peut correspondre plusieurs autres. Ainsi le décryptage se fait en suivant le bon sens de la phrase ou du mot.

Exemple :

Dans l'applet ci-contre, la lettre «a» sera chiffrée par "21" ou "27" ou "31" ou "40".
Le fait de proposer plusieurs options de substitution pour les lettres les plus usuelles bouleverse les fréquences dans le texte chiffré. Et puisqu' aucun symbole n'apparait plus souvent que les autres, le message sera plus résistant à la cryptanalyse.

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ **Transformations du chiffrement par blocs**

a) *Chiffrement par substitution*

***La substitution de polygrammes** consiste à substituer un groupe de caractères (polygramme) dans le message par un autre groupe de caractères .*
*Les exemples les plus célèbres sont les algorithmes de **PLAYFAIR** et de **HILL** inventés en 1854 et utilisés pendant le première guerre mondiale par les anglais.*
*On dispose les **25** lettres de l'alphabet (W exclu car inutile, on utilise V à la place) dans **une grille 5x5**, ce qui donne la clef. La variante anglaise consiste à garder le **W** et à fusionner **I** et **J**.*

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) Chiffrement par substitution

B	Y	D	G	Z
J	S	F	U	P
L	A	R	K	X
C	O	I	V	E
Q	N	M	H	T

Règle 1

B	Y	D	G	Z
J	S	F	U	P
L	A	R	K	X
C	O	I	V	E
Q	N	M	H	T

Règle 2

B	Y	D	G	Z
J	S	F	U	P
L	A	R	K	X
C	O	I	V	E
Q	N	M	H	T

Règle 3

On chiffre le texte par groupes de deux lettres (des bigrammes) en appliquant les règles suivantes:

1. ***Si les deux lettres sont sur les coins d'un rectangle, alors les lettres chiffrées sont sur les deux autres coins. Exemple OK devient VA, BI devient DC, GO devient YV. La première des deux lettres chiffrées est sur la même ligne que la première lettre claire.***

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ **Transformations du chiffrement par blocs**

a) *Chiffrement par substitution*

B	Y	D	G	Z
J	S	F	U	P
L	A	R	K	X
C	O	I	V	E
Q	N	M	H	T

Règle 1

B	Y	D	G	Z
J	**S**	**F**	U	P
L	A	R	K	X
C	O	I	V	E
Q	N	M	H	T

Règle 2

B	Y	**D**	G	Z
J	S	F	U	P
L	A	**R**	K	X
C	O	I	V	E
Q	N	**M**	H	T

Règle 3

2. *Si deux lettres sont sur la même ligne, on prend les deux lettres qui les suivent immédiatement à leur droite: **FJ** sera remplacé par **US**, **VE** par **EC**.*

3. *Si deux lettres sont sur la même colonne, on prend les deux lettres qui les suivent immédiatement en dessous: **BJ** sera remplacé par **JL**, **RM** par **ID**.*

4. *Si le **bigramme** est composé de deux fois la même lettre, on insère une nulle (usuellement le X) entre les deux pour éliminer ce doublon.*

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) *Chiffrement par transposition*

Les transpositions consistent à mélanger les symboles ou les groupes de symboles d'un message clair suivant des règles prédéfinies pour créer de la diffusion. Ces règles sont déterminées par la clé de chiffrement. Une suite de transpositions forment une permutation.

***Simple par bloc** On découpe le texte en blocs de m lettres puis on applique une permutation sur ces lettres en ne prenant en compte que la place qu'elle occupe. Ainsi par exemple, la première lettre du bloc va devenir la x ième, la seconde va devenir la y ième …(pour x ,y …différents les uns des autres et inférieurs à m bien sûr).*

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) *Chiffrement par transposition*

Exemple :
m=3, T(1)=3, T(2)=1 et T(3)=2 C'est à dire :

T	1	2	3
	3	1	2

Ainsi : MAT HEM ATI QUE S
Va devenir

M	A	T		H	E	M		A	T	I		Q	U	E		S
A	T	M		E	M	H		T	I	A		U	E	Q		S

ATM EMH TIA UEQ S

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) *Chiffrement par transposition*

Simple par colonnes *on écrit le message horizontalement dans une matrice prédéfinie, et on trouve le texte à chiffrer en lisant la grille verticalement (cf. la figure ci-dessous). Le destinataire légal pour décrypter le message réalise le procédé inverse.*

Exemple

Exemple : texte à chiffer = « I LOVE MY ENGLISH TEACHER »
utilise une matrice [6;4].

I	L	O	V
E	M	Y	E
N	G	L	I
S	H	T	E
A	C	H	E
R			

TRANSPOSITION SIMPLE PAR COLONNES

texte chiffré = « IENSA RLMGH COYLT HVEIE E »

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ **Transformations du chiffrement par blocs**

a) *Chiffrement par transposition*

Complexe par colonnes *un mot clé secret (avec uniquement des caractères différents) est utilisé pour dériver une séquence de chiffres commençant à 1 et finissant au nombre de lettres composant le mot clé. Cette séquence est obtenue en numérotant les lettres du mot clé en partant de la gauche vers la droite et en donnant l'ordre d'apparition dans l'alphabet. Une fois que le séquence de transposition est obtenue, on chiffre en écrivant d'abord le message par lignes dans un rectangle (comme le dessin ci-dessous le montre), puis on lit le texte par colonnes en suivant l'ordre déterminé par la séquence.*

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) *Chiffrement par transposition*

Exemple

Exemple : texte en clair = «I LOVE MY ENGLISH TEACHER»
utilise le mot clé **SERGIO.**

Clé :

S	E	R	G	I	O
6	1	5	2	3	4
I	L	O	V	E	M
Y	E	N	G	L	I
S	H	T	E	A	C
H	E	R			

TRANSPOSITION COMPLEXE
PAR COLONNES

texte chiffré = « LEHEV GEELA MICON TRIYS H »

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ **Transformations du chiffrement par blocs**

a) ***Chiffrement par transposition***

Par carré polybique *Fait à partir d'un carré de Polybe (Historien grec du II ème siècle av. J.C.), contenant toutes les lettres dans un ordre précis et pouvant être repérées chacune par deux coordonnées (on peut utiliser un mot clé précis pour faire ce carré, l'écrire dans la première ligne puis compléter le tableau avec les lettres manquantes dans l'ordre alphabétique). On écrit d'abord la première coordonnée de chaque lettre du message puis après à la suite la deuxième coordonnée de chaque lettre, et enfin on réunit par paire chaque coordonnée pour les transposer en une lettre grâce au tableau. (Par exemple la première lettre du message codé se trouve être la lettre ayant pour première coordonnée, la première coordonnée de la première lettre et pour deuxième coordonnée, la première coordonnée de la deuxième lettre).*

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑Transformations du chiffrement par blocs

a) *Chiffrement par transposition*

Exemple

	1	2	3	4	5
1	S	T	E	P	H
2	A	B	C	D	F
3	G	I	J	K	L
4	M	N	O	Q	R
5	U	V	W	X	Y
6	Z	.	;	,	!

	M	A	T	H	E	M	A	T	I	Q	U	E	S
1 ère coordonnée	4	2	1	1	1	4	2	1	3	4	5	1	1
2 ème coordonnée	1	1	2	5	3	1	1	2	2	4	1	3	1

Ce qui nous donne : 42 11 14 21 34 51 11 12 53 11 22 41 31

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique**

❑ **Transformations du chiffrement par blocs**

a) *Chiffrement par transposition*

Exemple

1 ère coordonnée	4	1	1	2	3	5	1	1	5	1	2	4	3
2 ème coordonnée	2	1	4	1	4	1	1	2	3	1	2	1	1
	N	S	P	A	K	U	S	T	W	S	B	M	G

On obtient au final : NSPAKUSTWSBMG

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique et asymétrique**

❑ **Algorithme symétrique**

a) ***Blowfish***

Blowfish a été conçu par Bruce Schneier en 1993 comme étant une alternative aux algorithmes existants, en étant rapide et gratuit.

Il utilise itérativement une fonction de chiffrement 16 fois.

La grandeur des blocs est de 64 bits.

Il peut prendre une longueur de clé variant entre 32 bits et 448 bits.

Sécurité des systèmes d'information

Abdelouahed Ennibi
Email: ennibi@gmail.com

I. Sécurité informatique

- Notions fondamentales de sécurité
  - **Cryptographie symétrique et asymétrique**

❑ **Algorithme symétrique**

a) DES (Data Encryption Standard)

L'algorithme DES, Data Encryption Standard, a été créé dans les laboratoires de la firme IBM Corp.

C'est un chiffrement qui transforme des blocs de 64 bits avec une clé secrète de 56 bits au moyen de permutations et de substitutions.