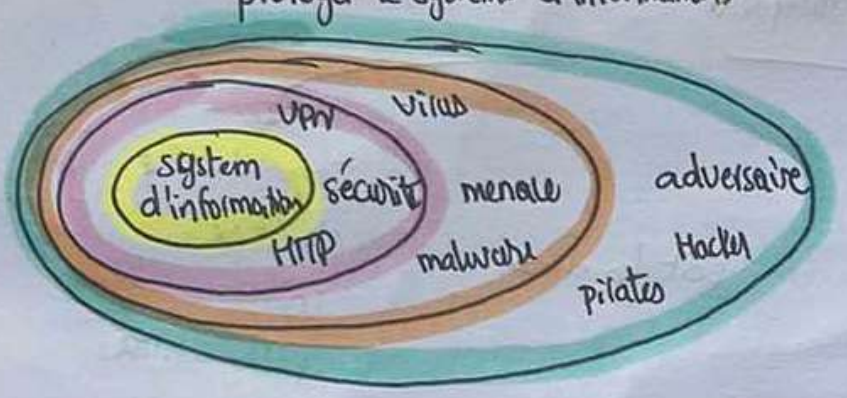
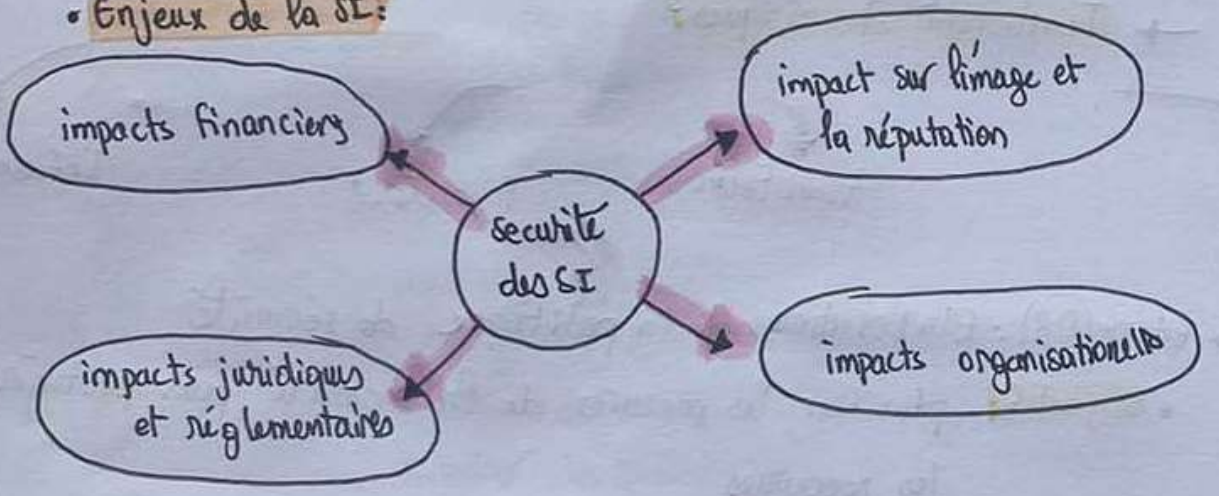
chapitre (01): Introduction à la sécurité

- Definition: Ensemble de moyens techniques, organisationnels et juridiques visant à protéger le système d'information.



- Enjeux de la SI:



- objectif de la SI:

TRIAD CID:

⬅ propriétés fondamentales de la sécurité

→ Confidentialité : préservé l'accès aux données aux seules personnes autorisés
→ Intégrité: garantir que les données ne soit pas modifiés de manière non autorisée
→ Disponibilité: Assurer l'accès aux ressources en temp utile.

objectif au-delà de CID:

- **identification:** (as signup) معلومات تعرّف بك
- **Authentification** (Signin) معلومات المستخدمة للتحقق من الهوية
- **autorisation** permission d'accéder à des choses spécifiques
- **non-répudiation:** garantie que une action ne peut pas être nié par la personne qui l'a effectuée ou qui été censée en recevoir
- **traçabilité** capacité de suivre et de retrouver toutes les actions effectuées sur les ressources de l'entreprise

• principaux concepts de SI:

- **Vulnérabilité:** faiblesse au niveau d'un bien (corona virus) (pas de masque)
- **menace:** cause potentielle d'un incident pourrait entraîner des dommages (corona virus)
- **Attaque:**
- **contre mesure:** l'ensemble des actions mises en oeuvre pour de miner ou éliminer le risque. (porter un masque)

• Système de management de SI:

→ **Definition:** système structuré de gestion de la sécurité de l'information

→ **Objectif:**

- Gérer les risques de sécurité informatique de manière efficace.
- Établir, mettre en oeuvre, surveiller, maintenir et améliorer la SI

→ **norme de cybersécurité:**

➡ **ISO 17799:** Guide de bonnes pratiques en SI

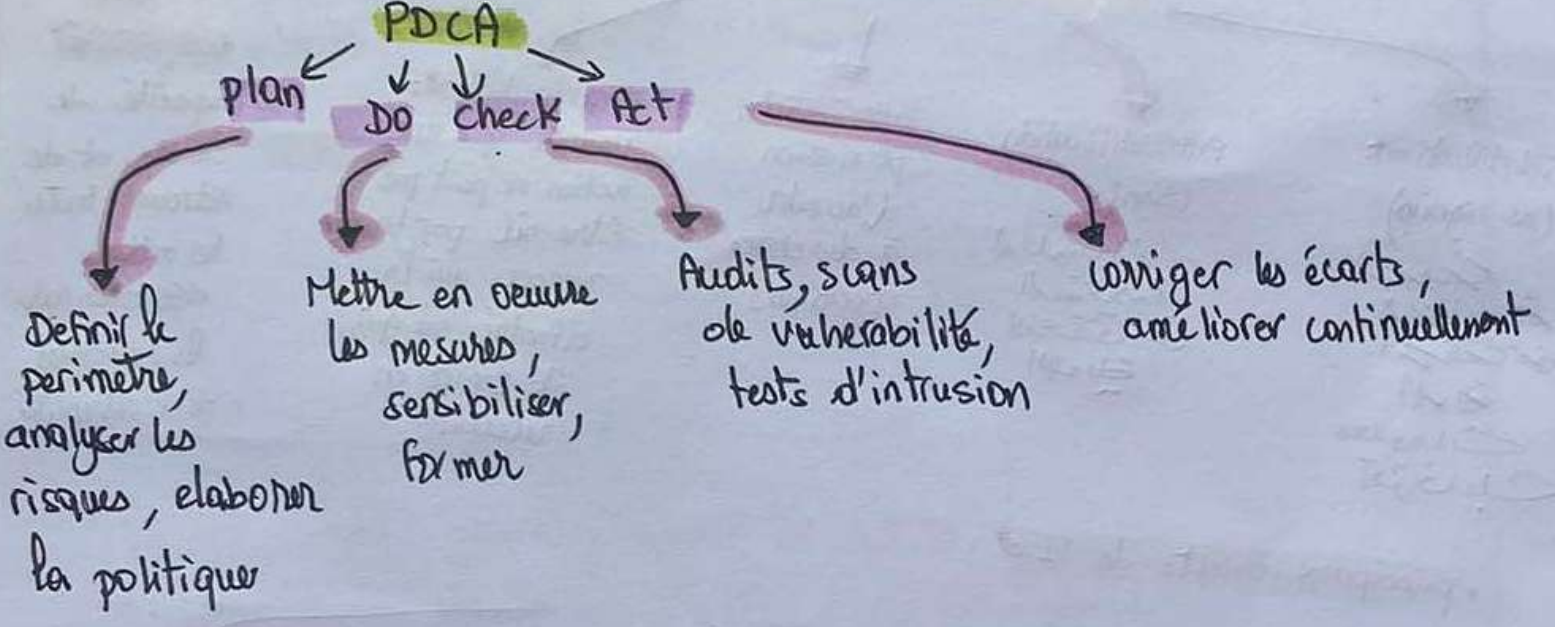
➡ **ISO 27000:** famille de normes pour la gestion de SI

➡ **ISO 27001:** specifie les exigences pour un SMSI

➡ **ISO 27005:** Gestion de risques

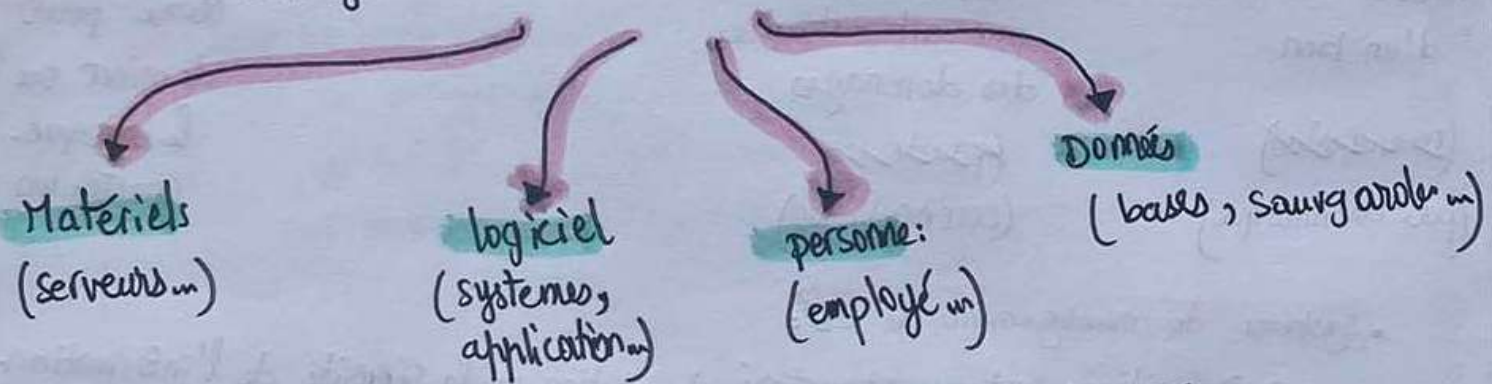
➡ **ISO 27002:** Mesures et contrôles de sécurité (bonnes pratiques)

→ ISO 27001 et Modèle PDCA



→ Etape 01: Définir le périmètre

- Délimiter ce que le SMSI couvre (activités, actifs, systèmes)
- classifier les actifs:



- objectif: identifier les éléments critiques à protéger.

→ Etape (02): Analyse des risques

Normes : EBIOS, MEHARI, OCTAVE, ISO 27005

→ Etapes:

① - Identification des actifs
② - " des vulnérabilités
③ - " des menaces
④ - Estimation d'impact
⑤ - probabilité d'occurence

risque = menace * vulnérabilité * impact

probabilité d'occurence

→ Estimation du risque :

Qualitatif :
faible
moyen
fort

soit les deux

Quantitatif :
chiffre
coût
perte estimée

→ Traitement des risques :

Réduire

transférer

Accepter

Refuser

→ Etape(03) : Elaboration de la politique de sécurité

• objectif : planifier les mesures de la sécurité pour protéger les ressources

inclure :

Standard :
(ISO, ANSSI)

Guide :
(bonne pratique)

procédure :
(techniques precises)

procédure : pose le cadre et les objectifs

politique : detaille les étapes et les moyens techniques attendre ces objectifs

➡ Etape (04): Mise en oeuvre (DO)

- application concrète de la politique de sécurité
- action:
  - → former et sensibiliser le personnel.
  - → Déployer les controles de sécurité (pare-feu, anti-virus)
  - → Appliquer les procedures définies

➡ Etape (05): Verification (check)

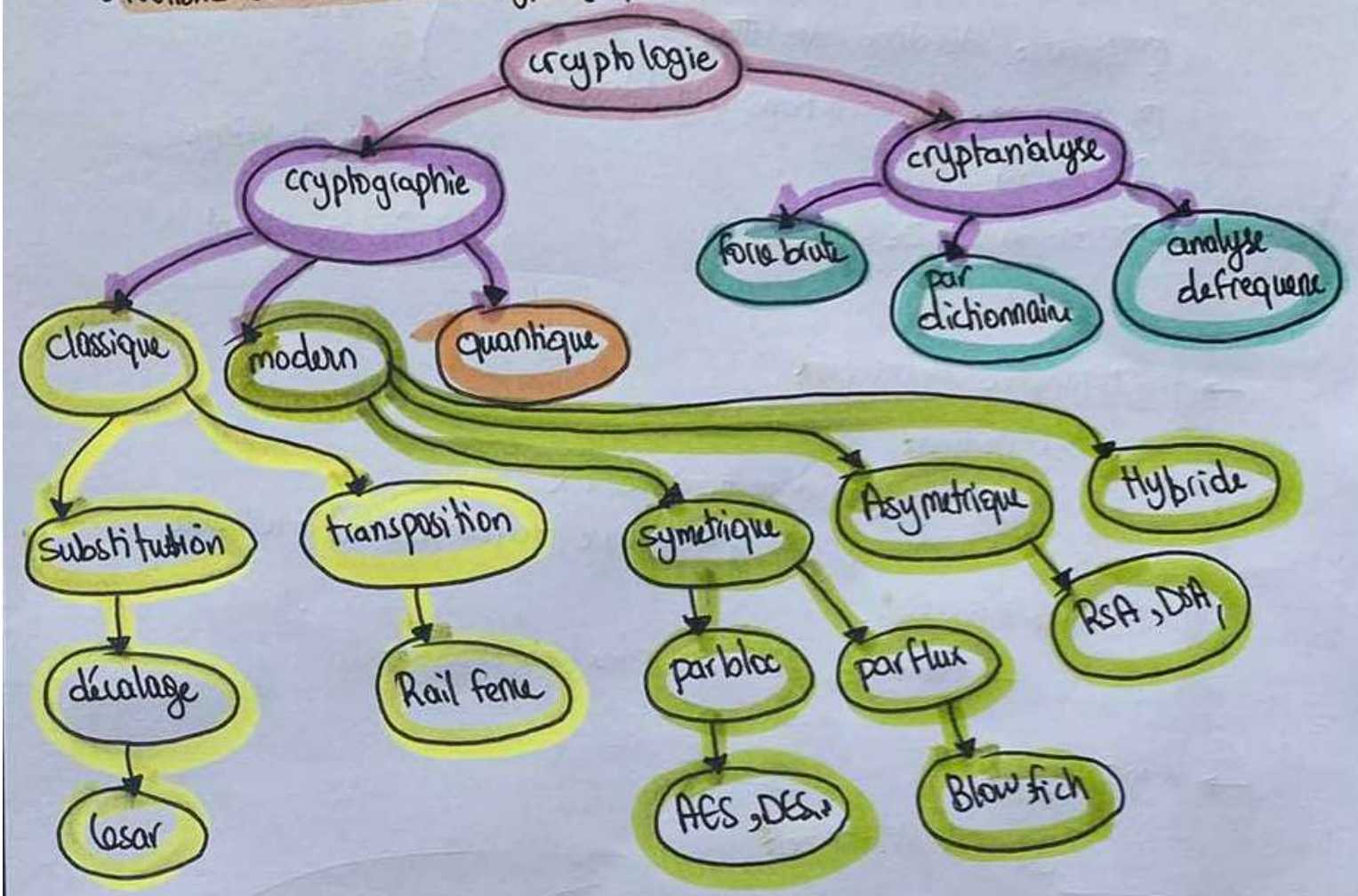
- Contrôle de l'éfficacité du système
  - → Audit de sécurité (مراجعة)
  - → Scans de vulnerabilités
  - → tests d'intrusion

➡ Etape (06): Amélioration (Act)

- sur la base des audits:
  - → corriger les écarts
  - → Ajouter de novelles mesures
  - → Adapter la politique aux nouvelles menaces

chapitre (01): Introduction à la cryptographie

- Notions de bases de la cryptographie :



- Définitions de base:
  - cryptographie: chiffrer le message
  - cryptanalyse: casser le système de cryptographie
  - cryptologie = cryptographie + cryptanalyse
  - cryptosysteme = ensemble des fonctions de chif/dechif + clés

- objectifs de la cryptographie:

confidentialité — integrité — Authentification — non-repudiation

- Histoire:
  1. scytale: message autour d'un bâton
  2. Cesar: décalage des lettres
  3. Vigenere: subtitution polyalphabetique
  4. Enigma
  5. Modome: DES/AES.

} âge artisanal
} âge technique
} âge paradoxal

→ cryptographie classique:

- subtitution:
  → décalage d'un nombre fix
  → facile a cassé par analyse fiequentielle ou force brute
- trans posision:
  → Mélange des lettres sans en changer

→ cryptanalyse

Type d'attaquee:

force brute: tester tout les clé possibles

Analyse fiequentielle: basé sur la fréquence des lettres

indice de coicidence:

text clair connu / choisis, text chiffré choisi (selon les capacités de l'attaquant) (c'est l'attaque par dictionnaire)

methode Kaiski → indice de coisidence → Analyse frequentielle

$$ic = \sum \frac{fi(fi-1)}{N(N-1)}$$

→ chifferement par transposition:

- Columnar:
  message: "message confidentiel"
  clé = 5

m	e	s	s	a
g	e	c	o	n
f	i	d	e	n
t	i	e	l	

message chiffré : mgfte eeii soel ann Capres E → S → U

- **Keyword Columnar :**

M : un message confidentiel

clé : secu

Message chiffré : ma ode nscii useft
egnel

clé	S	E	C	U
/	3	2	1	4
/	u	n	m	e
/	s	s	a	g
/	e	c	o	n
/	f	i	d	e
/	t	i	e	l
/			1	

→ **clé faible :**

dans cesar, c'est la clé ou on chiffre le message deux fois on obtient le message claire

- **Cryptographie modern :**
  - Manipule des bits (non pas des lettres)
  - toujour basé sur sublitution et transposition, mais de façon plus complexe
  - → **objectif :** même avec du texte chiffré accessible, aucune information ne doit être déductible sans la clé.

- **cryptographie symétrique :**
  - → même clé pour chiffré et déchiffrer ($K_e = K_d = K$)
  - → necessite un canal sécurisé pour l'échange de clé.
  - → Rapide, mais la distribution des clé devient complexe à grande echelle.

type

chifferement par bloc :
devise le message en blocs
(AES, DES)

chifferement par flux :
bit à bit, un octet par octet

→ Chiffrement par blocs :

Concepts de shanon :

→ **confusion :** relation entre clé et message chiffré n'est pas clair

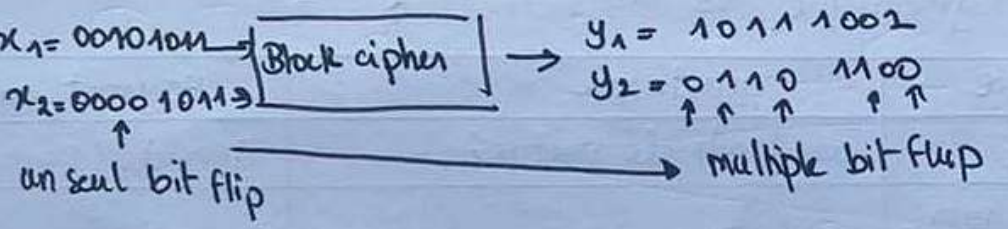
→ **Diffusion :** un petit changement dans message clair → grands changements dans le message chiffré.

fonctionnement :

→ combinaison de plusieurs tours de substitution + transposition

→ clé souvent ⩾ 128 bits (DES : 56 bits, AES jusqu'a 256 bits)

Exemple Diffusion :



→ DES (Data Encryption standard)

fonctionnement : chifferement par blocs de 64 bits avec une clé de 56 bits et 16 tours (~~transpos~~ transposition et substitution) utilisant un réseau de Fiestel

sécurité : obsolète car sa clé courte le rend vulnérable aux attaque par force brute.

S-DES (DES simplifier) : version simplifier de DES pour l'apprentissage (blocs 8 bits, clé 10 bits, 2 tours)

→ AES (Advanced Encryption standard)

fonctionnement : chifferement par blocs de 128 bits avec des clés de 128, 192, 256 bits et 10, 12, 14 tours selon la taille de la clé (128 → 10, 192 → 12 256 → 14)

⇝ utilise SubBytes, ShiftRows, MixColumns, AddRoundKey

- SubBytes : Remplace chaque octet par un autre via une table (S-Box)
- ShiftRows : Décale circulairement les lignes d'une matrice
- MixColumns : Mélange linéairement les colonnes d'une matrice
- AddRoundedKey : XOR entre la matrice et une sous clé

Sécurité : très forte (standard actuel)

→ Mode de chiffrement par blocs :

- ECB : chaque bloc chiffré indépendamment (faible)
- CBC : chaque bloc est XORé avec le précident + IV

vecteur d'initialisation, bloc de bits aléatoire ou pseudo aléatoire pour initialiser un algo de chifferement (non secret)

- CFB, OFB, CTR : modes "flux" utilisant IV, adapté a ces cas specifiques

↝ IV doit être unique à chaque chifferement

→ problèmes de la cryptographie symétrique :

- Distribution des clés : pour n personnes → $n((n-2))/2$ clés nécessaires
- Difficile a géré à grande échelle.

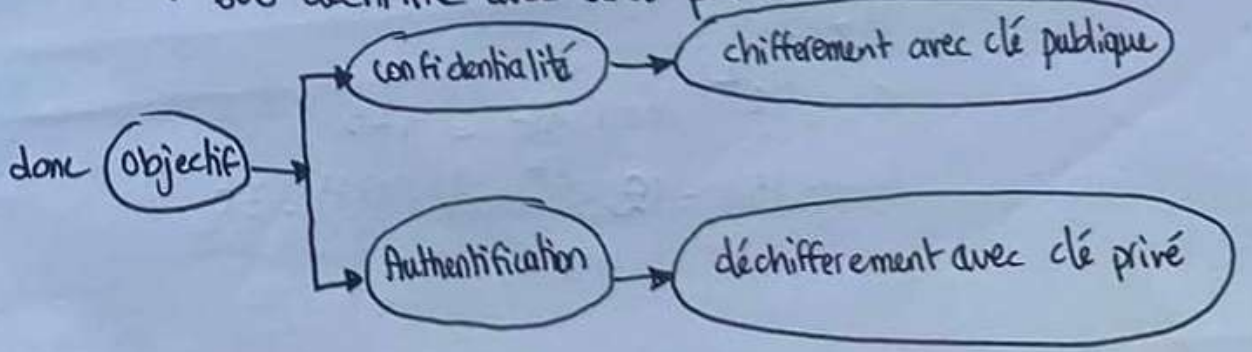
- Cryptographie Asymétrique : (à clé publique)

principe :

→ Deux clés : publique pour chiffrer et privé pour déchiffrer

fonctionnement :

→ Alice chiffre avec clé publique de Bob (chaqu'un a ces clés publique et privé)
→ Bob dechiffre avec sa clé privé



→ signature numérique : (authentification)
propriétés : Authentique, non falsifiable, non réutilisable, non répudiable, inaltérable.

→ Algorithme RSA :

→ Basé sur une fonction unidirectionnelle à trappe :
facile à faire dans un sens, mais impossible à inverser sans la trappe (clé privé)

→ Etapes de génération des clés RSA :

① - choisir deux nombres premiers p et q

② - calculer tq : $n = q * p$ et $\phi(n) = (p-1) * (q-1)$

③ - choisir un e tq : $1 < e < \phi(n)$ et $PGCD(e, \phi(n)) = 1$

④ - calculer d tq : $d \equiv e^{-1} \mod (\phi(n))$ (inverse de e mod $(\phi(n))$)

→ clé RSA :
- publique (e, n)
- privé (d, n)

→ fonction :
chiffrement : $C = M^e \mod n$
déchiffrement : $M = C^d \mod n$

exemple : $p = 17$, $q = 11$ → $n = 187$, $\phi(n) = 160$, $e = 7$
$d = 23$
clé publique $(7, 187)$
clé privé $(23, 187)$
$M = 30$
$C = 30^7 \mod 187 = 123$
déchiffrer $= 123^{23} \mod (187) = 30$

→ Avantages et inconvénients :

→ Avantages :

- plus besoin d'échanger une clé de secrète
- permet l'authentification et la non-répudiation

→ Inconvénient :

- lent pour grande message
- Nécessite des clés longues
- on chiffre généralement un petit message (clé de session), pas toute le fichier.

Symétrique VS Asymétrique :

critère	Symétrique	Asymétrique
clé	une seule clé partagé	Deux clé (privé, Publique)
clés à gerer (n personnes)	$n(n-1)/2$ clé	n paires clés
échange de clé	Necessaire, canal sécurisé	Non nécessaire (clé publique)
Vitesse	80 à 256 bits	512 à 4096 bits
Usage	chifferement rapide des données	Échange de clé, signature, authentification

→ fonction de Hashage :

- transforme les données de taille variable en une empreinte fixe (ex : 256 bits)
- Sens unique : on ne peut pas trouver les données de l'origine
- Utiliser pour : intégrité, signature numérique, vérification

→ Exemple : SHA 1, SHA-2 ...

→ Signature numérique :

- garantir → Authenticité
  → Intégrité
  → Non-répudiation
- Réaliser avec clé privé et vérifier avec clé publique
- On signe le hashage du message pour gagner du temps

→ Risque : attaque Man-in the-Middle (MITM):
- un attaquant peut remplacer la clé publique.
- Nécessite d'un certificat électronique signé par une autorité de confiance (AC)

→ certificat électronique:
- fichier signé par une autorité de confiance, contenant:
  - clé publique
  - identité du propiétaire (nom, adresse, ... etc)
  - la signature de l'autorité (AC)
- utilité:
  → Associer une clé publique à une identité
  → prévenir les attaques MITM

→ Gestion de clés publiques : PK

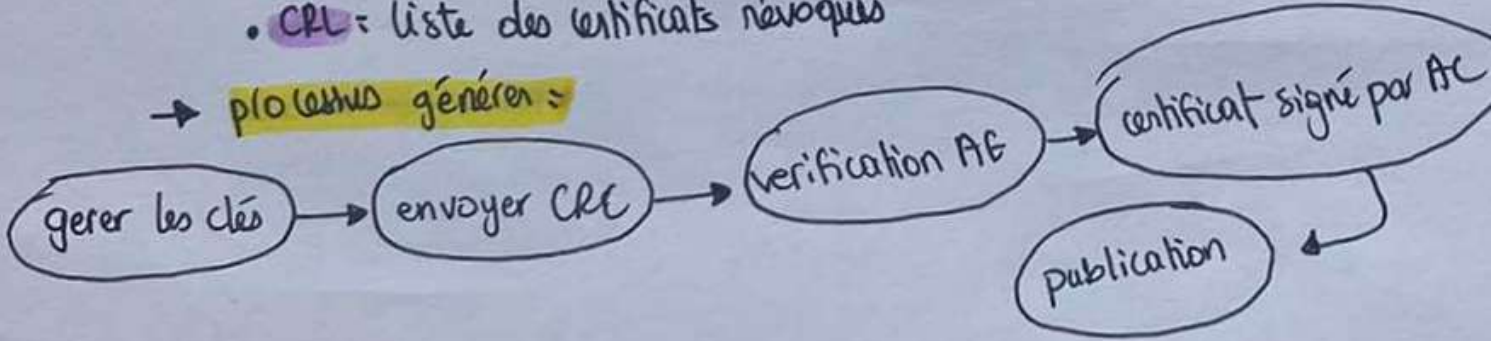
PKI:
(hiérarchique, avec autorité de ~~confiance~~ certificat)

→ PKIX: norme PKI basé sur certificats X.509
  → Gère: création, publication ... etc de certificats
  → permet de faire confiance à une clé publique via une chaîne de certificats

Web of trust:
(non hierarchique, confiance entre utilisateurs)

→ composants clés:
- AE: (Autorité d'enregistrement): vérifier les demandes et identités
- AC: émet, signe, révoque les certificats
- CSR: demande des certificats
- CRL: liste des certificats révoqués

→ processus générer:



→ **chaine de confiance:** certificat utilisateur, signé par CA intermédiaire, lui même signé par CA racine

→ **Services AC:** إلغاء

- creation, publication, renouvellement et révocation des certificats
- **Raison de révocation:**
  - clé compromise (مخترق)
  - Perte de role
  - compromission de AC

- الملكية
- الحيازة

→ **Role de AE:** vérification identité, preuve de possession, gestion de la clé privée.